G DATA ANTIVIRUS

ユーザーマニュアル

目次

はじめに

この度はG DATA 製品をお買い求めいただき、誠にありがとうございます。本マニュアルでは、製品のインストール、コンピュータを不正プログラムから効果的に保護するためのヒントが分かりやすく纏められています。本製品を操作する上でわからないことがでてきたら、まずは、マニュアルやG DATA ウェブサイトのFAQなどでご確認ください。

このマニュアルでは、製品のインストール方法と実用的なヒントをまとめています。

*スクリーンショットに関して: 本マニュアルで使用されている画像は、開発中のトータルプロテクションを使用しています。

メモ: 各機能の使用方法を簡単に調べたい場合はオンラインヘルプが便利です。オンラインヘルプは各画面にあるヘルプボタンを押すことで表示できます。

ユーザーサポートについて

操作方法など、ご購入後の製品に関するお問い合わせは、ユーザーサポートで受付いたします。

※体験版の場合は、ユーザーサポートのご利用はできません。予めご了承ください。

ユーザーサポートの連絡先

問い合わせ先については、登録後のメールをご確認ください。

1. サポート期間

ライセンス有効期間内

2. サポート範囲

製品のご利用の説明、疑問点にお答えするサービスとさせていただきます。
以下の場合には、お問い合わせに対してのご回答ができませんので、予めご了承ください。

a) 本製品で保証している動作環境外でのお問い合わせ
b) 本製品ではないもの（ハードウェア・他社製品）に関するお問い合わせ
c) サポート時間外のサポートおよび、指定された方法以外の方法でのサポートのご依頼

3. ユーザーサポートをお受けになる際に
お問い合わせの際は、お客様番号または、レジストレーション番号をご用意いただき、更に質問要点を整理していただいた上で、お問い合わせいただきますようお願いいたします。

インストール

まず本製品をインストールする環境についてご確認ください。本製品を正常に機能させるためには、以下の**動作環境**を満たす必要があります。

動作環境

対応OS	Windows 10 (32bit/64bit) Windows 8/8.1 (32bit/64bit) Windows 7 (32bit/64bit) Windows Vista (32bit/64bit) Windows XP [SP2以降](32bit) ※インストールには管理者(Administrator)権限でログインする必要があります。 ※日本語OS環境のみサポート。 ※最新のサービスパックを推奨。
CPU	各OSが推奨するCPU

メモリ	Windows 10/8/8.1/7/Vista：1GB以上 [2GB以上推奨] Windows XP：512MB以上 [1GB以上推奨] ※グラフィックメモリとの共用は除きます。
ハードディスク	1GB以上の空き容量
デバイス装置	CDドライブ（パッケージ版のみインストール時に必要） ※ブートCDの作成・バックアップ時には書き込み可能なCD/DVDドライブが必要です。
ディスプレイ	解像度1024×768ドット、High Color（16ビット、65,536色）以上
その他	InternetExplorer8以上 インターネットに接続可能な環境[ブロードバンド以上を推奨]

※他のウイルス対策ソフトとは併用できません。
※ユーザー登録するためにはPCのメールアドレス（携帯メール不可）が必要です。
新品のコンピュータ、もしくは本製品インストール前に他のウイルス対策ソフトで保護されていたコンピュータでは、次のステップを参考に本製品をインストールしてください。それ以外の場合やコンピュータがウイルスに感染している疑いがある場合は、インストール前にブートスキャンを実行することをお勧めします。 ブートスキャンの方法については、ブートスキャンの流れを参照してください。

注意: 本製品をインストールしようとしているコンピュータに、他社製のウイルス対策ソフトがインストールされている場合は、**必ず他社製品をアンインストールした後で、本製品をインストールしてください。**ウイルス対策ソフトは Windows のシステム深くに配置されて動作するため、複数の製品を同時に使用すると深刻な問題が出る場合があります。
なお、他社製品をアンインストールする場合、通常アンインストールではデータのゴミが残る場合がほとんどで、動作不良の原因となります。製品ごとに用意されている、**完全アンインストールツール**を使用してアンインストールする事で、コンピュータをクリーンな状態にでき、その上で本製品をインストールする事で最適な動作をさせることができます。他社製品の完全アンインストールツールに関しては、各社のユーザーサポートをご利用ください。

ステップ1 - インストールの開始

本製品はCD/DVD版もしくは、ダウンロード版として販売されています。それぞれのインストール方法は次の通りです:

- **CD/DVD 版の場合**: 本製品CD/DVDをドライブにセットします。
- **ダウンロード版の場合**: ダウンロードしたファイルをダブルクリックします。

しばらくすると、自動的にインストール開始画面が開きます。

> **注意**: インストール起動画面が自動表示されない場合は、Windowsの自動再生機能が無効になっている可能性があります。
>
> - 自動再生の画面が表示される場合は、**AUTOSTRT.EXE の実行** をクリックしてください。
> - 自動再生の画面が開かない場合は、Windows 上で本製品のディスクを探して開き、**Setup** もしくは **Setup.exe** をダブルクリックしてください。

ステップ2 - インストール方法の選択

ウィザードに沿ってインストールを行います。まず、**標準インストール**もしくはユーザー自身でインストール内容を決定できる**カスタムインストール**を選択する画面が表示されるので、希望するインストール方法を選択してください。（推奨: 標準インストール）

> カスタムインストールでは、プログラムの保存場所やインストールする機能を任意で選択できます。

- 標準インストールを選択した場合

  ステップ3の画面が表示されます。

- カスタムインストールを選択した場合

  使用許諾契約の画面が表示されるので、**使用許諾契約の条項に同意します**にチェックを入れて［次へ］を選択します。ステップ4のカスタムインストール用の画面が表示されます。

マルウェア情報イニシアチブとは

G DATA セキュリティラボでは、G DATA 製品の利用者をコンピュータの安全性を脅かす脅威から保護するため、保護・対策の研究や分析に絶え間なく励んでいます。 マルウェア研究では、マルウェアに関する情報が多ければ多いほど、効果的な保護メカニズムの開発をいち早く進めることができます。これらの情報をG DATAの研究・分析・開発に効率的に取り入れることを可能にするための取り組みが、G DATA マルウェア情報イニシアチブです。 これにより、マルウェアに関するデータをG DATA セキュリティラボに送信することができます。 より多くのユーザー様に参加頂くことで、他のG DATA 製品をご利用の方々もインターネットをより安全に利用できるようになります。このインストール方法の選択画面にあるチェックボックスで、このデータを提供するかどうかの選択ができます。

ステップ3 - 使用許諾契約

使用許諾契約書をご確認いただき、同意できる場合は［**同意してインストール**］をクリックしてください。インストールが始まります。

ステップ4 - カスタムインストール (オプション)

カスタムインストールを選択した場合は、次の2つの画面で**インストール先フォルダ**と**インストールする機能の範囲**を指定します。
標準インストールを選択した場合は、この手順は省略されます。

あらかじめ設定されているインストール範囲には以下の違いがあります。

- **ユーザー定義**: この設定ではソフトウェアの機能（例: アンチウイルス、アンチスパムなど）の横にあるボックスをチェックして、インストールする機能を自分で指定することができます。G DATA アンチウイルス、G DATA インターネットセキュリティ、またはG DATA トータルプロテクション、それぞれの製品に応じて、ここで選択できる機能の種類は変わります。

- **完全**: 製品に含まれる全ての機能がインストールされます。

- **最小**: ウイルス対策に最低限必要な、アンチウイルス機能のみがインストールされます。

本製品のインストール後に、あとからインストールされている機能を変更する事も可能です。セットアップを起動し、**変更**を選択すると、カスタムインストールの要領で機能の追加や削除を行う事ができます。

ステップ5 - 製品種類の選択

この手順では、本製品を製品版として使用するか、体験版として試用するかを選択します。

- **製品版として登録**: 製品版を購入した場合は、ここを選択します。

- **体験版として登録**: 無料体験版として利用する場合は、ここを選択します。なお、体験版を利用するには、氏名とメールアドレスの入力が必要です。入力されたメールアドレスには、アクセスデータが送付されるので、必ず有効なPC用メールアドレスを入力してください。

ステップ6 - ライセンスの認証

インストール中に**ライセンスの認証**を行い、プログラムの機能をすべて使用できるようにします。

- **レジストレーション番号を入力**: 製品を新規購入された方は、ここを選択し、購入した製品のレジストレーション番号を入力してください。パッケージ版を購入された場合は、レジストレーション番号は同梱の用紙に記載されています。ダウンロード版を購入された場合は、レジストレーション番号はメールなどで送信されています（購入したWEBストアによって異なります）。

  注意: レジストレーション番号を入力して、製品が正常に認証されると、更新ファイルをロードできるようになります。複数台版やライセンスの移行で必要になるアクセスデータは、認証後に G DATA から送付されるメールに記載されています。アクセスデータは厳重に保管してください。

  入力したレジストレーション番号で認証できない場合は、まず入力ミスの可能性がないか確認してください。それでも問題が解決できない場合は、ユーザーサポートにお問い合わせください。

- **アクセスデータを入力**: アクセスデータ（ユーザー名とパスワード）を使って、認証します。本製品を再インストールしたり、他のコンピュータでライセンスを認証したい場合（複数ユーザー版の場合など）は、ここを選択してアクセスデータを入力してください。

  注意: アクセスデータは初回認証（レジストレーション番号を入力）後に G DATA から送付されたメールに記載されています。製品には同梱されていません。

  アクセスデータを紛失したり忘れた場合は、**アクセスデータの確認**をクリックしてください。ブラウザが自動的に起動して G DATA のサポートページが開きます。サポートページに記載されている手順に沿って手続きをし、アクセスデータを再確認してください。※アクセスデータの再確認では、レジストレーション番号が必要です。またレジストレーション番号の登録時に使用したメールアドレスを変更した場合は、ユーザーサポートへお問い合わせください。

- **後で認証を行う**: 後で製品を認証する場合はここを選択します。認証を行わない場合はワクチン更新が行われないため、最新の脅威に対して適切な保護を提供する事ができなくなります。インストール後はできるだけ早く認証の手続きをしてください。インストール後の認証は、ワクチン更新を実行しようとした際に表示されるウインドウか、設定アイコンをクリックして、**アンチウイルス**の**更新**領域などから行う事ができます。

ステップ7 - インストールの完了

最後に、インストールを完了するためにコンピュータを再起動してください。再起動が完了すると本製品が使用可能になります。

インストール後

インストール後には、ショートカットやタスクバーのアイコンから本製品を起動できるようになり、各種セキュリティ機能が利用可能になります。

G DATA ショートカット: 左のアイコンがデスクトップ上に作成されます。本製品のインターフェースを開くには、このアイコンをダブルクリックします。セキュリティセンターの利用方法については、セキュリティセンターに詳しく記載しています。

G DATA アイコン: ユーザーの操作が必要になると、タスクバーのG DATA アイコンからお知らせします。このアイコンを右クリックして起動を選択する事で G DATA のインターフェイスを開く事ができます。その他の情報は、G DATA アイコンの項を参照して

ください。

G DATA シュレッダー: インストールでシュレッダーを選択すると、デスクトップ上にシュレッダーアイコンが作成されます。シュレッダーを使ってファイルを完全に削除するには、ファイルをシュレッダーのアイコン上に移動するか、ファイルの上で右クリックして、シュレッダーを選択します。一旦シュレッダーでファイルを削除すると、ファイルは復元不可能になります。※シュレッダー機能は、**G DATA アンチウイルス**には含まれていません。

クイックスキャン: 特定のファイルやフォルダだけをウイルススキャンしたい場合は、プログラム画面を起動する必要はありません。対象の上で右クリックし、**ウイルススキャン**を選択すると、スキャンが実行されます。

本製品をインストールしてコンピュータを再起動した際に、Windows が起動しない場合: まずCD/DVDドライブに本製品CDが挿入されたままではないか確認してください。本製品CDは、ブートスキャン機能を搭載しているので、コンピュータの設定によっては、Windows 起動前にブートCD が起動している可能性があります。製品CDがCD/DVDドライブに挿入されていた場合は、CDを取り出し、コンピュータを再起動してください。Windows が通常通りに起動します。

ブートスキャンに関する詳細は、**ブートスキャンの流れ**の項を参照してください。

セキュリティセンター

本製品を起動すると立ち上がるセキュリティセンター画面では、各機能のステータスを確認したり、操作を実行できます。ウイルスなどの脅威に対する保護は、通常バックグラウンドで動作しますが、利用者の判断が必要になる場合はタスクバー上にその情報が表示されます。

セキュリティステータス

セキュリティステータスのアイコンを使用すると、ボタン操作ひとつでコンピュータの保護状況を簡単に改善できます。

このアイコンをクリックすると、コンピュータを守るための対策が提案されます。全てのセキュリティステータスが再び緑色に戻るまで対策を行い、保護レベルを改善してください。セキュリティステータスが全て緑色になれば、コンピュータの保護は最新の状態であり、セキュリティセンターでの作業も終了です。

緑色のチェックマーク＝すべて良好（システムは保護されています）

赤色のマーク＝今すぐに改善が必要（システムが危険にさらされている可能性があります）

灰色のマーク＝このセキュリティ機能は無効（例 アンチスパム機能を停止している）

黄色のマーク＝近いうちに改善が必要（例 ソフトウェアアップデートが利用可能）

本製品の全ての機能は、必要に応じて設定変更する事ができます。機能や設定の詳細については

このオンラインヘルプの各項目をご覧ください

ステータス

以下の項目から現在のセキュリティステータスの確認ができ、それぞれの項目をクリックし操作を実行することで、コンピュータの保護状況を改善できます:

リアルタイム保護

ウイルスガードはウイルスを常時監視するリアルタイムスキャン機能で、書き込みおよび読み取り処理を監視します。あるプログラムが不正な機能を実行したり、不正ファイルを拡散しようとすると、ウイルスガードがこれを防ぎます。ウイルスガードは最も重要なウイルス対策の１つですので、特別な理由が無い限り、常に有効にしておいてください。

- **ウイルスガードを無効にする**: 必要に応じてウイルスガードを無効化できます。例えば、大量のデータをハードディスク上のある場所から別の場所にコピーしたり、多くのメモリを必要とする演算プロセス（DVD のコピーなど）を実行する時には、ウイルスガードを無効にするとコンピュータのパフォーマンスが向上します。
  ただし、パフォーマンスのためにウイルスガードを無効化したい場合は、ウイルスガードを無効化する際や、アンチウイルスの設定画面から設定できる、セキュリティ / パフォーマンス のオプションを調整する事で、納得行くパフォーマンスを出せるか先に確認することをお勧めします。

  注意: ウイルスガードは必要な時だけ無効化してください。また、ウイルスガードが無効に設定されている間は、できるだけインターネットには接続しないようにし、CD、DVD、メモリカードまたは USB メモリなどに保存されている、スキャンをしたことのないデータにはアクセスしないように注意してください。

- **ふるまい検知を無効にする**: ふるまい検知（ビヘイビアブロッキング）は、ワクチンによる検出とは独立した、未知のウイルスを検出するための機能です。この機能は特別な理由が無い限り、常に有効にしておいてください。

- **詳細設定**: この機能に関する設定画面、設定 | アンチウイルス | リアルタイム保護 を開きます。

前回のアイドリングスキャン

前回コンピュータをアイドリングスキャンによってスキャンした日時が表示されます。この項目が赤色で表示されている場合は、できるだけ早くウイルススキャンを実行してください。※アイドリングスキャンが無効になっている場合は**前回のウイルススキャン**と表示されます。

- **コンピュータをスキャン**: コンピュータを数時間使わなくてもいい場合や、ウイルス感染の疑いがあり、すぐに結果を確認したい、といった場合には、ここからすぐにコンピュータ全体をスキャンできます。この全体スキャンの間もコンピュータは使用できますが、こ

こで実行されるスキャンはコンピュータの最大パフォーマンスを利用するため、他のアプリケーションのパフォーマンスにも影響を与えます。この機能の詳細は ウイルススキャンの流れ の項を参照してください。

- **今すぐ実行**: アイドリングスキャンは、ウイルススキャンがユーザーの作業の邪魔にならないように、コンピュータが使われていない状態にのみ自動的に起動するスキャン機能です。アイドリングスキャン中にユーザーがコンピュータを利用すると、実行中のスキャンはすぐに休止状態となります。次のアイドリングスキャン実行日よりも先にスキャンを行いたい場合は、**今すぐ実行**を選択してください。
仕事の休憩中などにアイドリングスキャンを自動実行したくない場合は、**アイドリングスキャンを無効にする**を選択して機能を無効化してください（非推奨）。

ウェブ保護

インターネット利用中の保護を提供する**ウェブ保護**の有効／無効を切り替えます。ウェブ経由での感染が増加している現在、ウェブ保護は感染防止のための重要な機能です。ウェブ機能を有効にすると、ウェブサイト経由の感染やフィッシング詐欺などの脅威をアクセス前に未然に防ぎます。

インターネット閲覧中にウェブサイトが本製品によって脅威として検出されると、サイトの閲覧はブロックされ、ブラウザ画面に警告が表示されます。

- **ウェブ保護を無効にする**: ウェブ保護を無効にすると、ウェブサイトのチェックが無効になるため、ウェブサイトから大量にデータをダウンロードする際などにダウンロード時間を省略できます。また、ウェブ保護が無効中の状態も、ウイルスガードがコンピュータを感染から守ります。しかし、例外的ケースを除いては、ウェブ保護は有効に設定することをお勧めします。

- **例外を設定**: ウェブ保護は、不正コードが仕掛けられたウェブサイト、またはフィッシングなどの詐欺サイトからコンピュータを保護する機能です。しかし場合によっては、ウェブ保護を有効にすると、安全なサイトであるにも関わらず、ウェブページが正しく表示されないことがあります。そのような場合は、対象ページのアドレスをホワイトリストに例外登録してください。これにより、ウェブ保護がブロックしていたページが閲覧できるようになります。詳細については、例外の項を参照してください。

- **詳細設定**: この機能に関する設定画面、設定 | アンチウイルス | ウェブ保護 を開きます。

メール保護

メール保護機能は、送受信されるメールの内容や添付ファイルをスキャンし、ウイルス感染を防ぎます。ウイルスが検出された場合は添付ファイルを削除、もしくはウイルスの駆除を行います。

- **メール保護を無効にする**: メールのスキャンを行いたくない場合は、ここを選択してください。ただし、その場合はメール経由のセキュリティリスクが大きく増えますので、特別な場合を除いてメール保護は有効に設定しておくことをお勧めします。

- **詳細設定**: この機能に関する設定画面、設定 | アンチウイルス | メールスキャン を開きます。

Microsoft Outlook: Microsoft Outlook には、専用プラグインがインストールされます。このプラグインは、メールスキャンで設定できる POP3/IMAP ベースの保護を提供し、これにより、Outlook 上でのウイルスチェックがより簡単に行えます。メールまたはフォルダのスキャンを実行するには、Outlook メニューバーの **[G DATA] > [フォルダをスキャン]** を選択します。
※通常のメールスキャンと併用すると送受信に問題が出る場合がありますので、その際はPOP/IMAP/SMTPのスキャンを無効にしてください。

前回のワクチン更新

ここでは、最後にインターネットからワクチンをダウンロードした日時が表示されます。ステータス情報が赤色で表示される場合には、できるだけ近いうちに、ワクチン更新を実行してください。ワクチンを更新するには、この項目をクリックし、プルダウン表示される**ワクチンの更新**を選択します。

- **ワクチンの更新**: デフォルト設定では、ワクチンの自動更新が行われように設定されています。今すぐに更新を手動実行する場合は、ここをクリックします。

- **自動更新を無効にする**: ワクチンの自動更新を無効にする場合はここをクリックします。特種なケースを除いて、自動更新は常に有効にしておいてください。

- **詳細設定**: この機能に関する設定画面、設定 | アンチウイルス | 更新 を開きます。

次回のワクチン更新

ここには、次回のワクチン更新までの時間が表示されます。ワクチンを更新するには、この項目をクリックし、プルダウン表示される**ワクチンの更新**を選択します。

- **ワクチンの更新**: デフォルト設定では、ワクチンの自動更新が行われように設定されています。今すぐに更新を手動実行する場合は、ここをクリックします。

- **自動更新を無効にする**: ワクチンの自動更新を無効にする場合はここをクリックします。特種なケースを除いて、自動更新は常に有効にしておいてください。

- **詳細設定**: この機能に関する設定画面、設定 | アンチウイルス | 更新 を開きます。

ライセンス

ワクチン更新が利用できるライセンスの有効期限を確認できます。

ウイルス対策ソフトにおいて、更新は非常に重要です。インターネット更新は必ず定期的に実行し、製品を常に最新の状態に保つように心がけてください。本製品はお手元のライセンスの有効期間が切れる前に、自動的にライセンス延長についてお知らせします。ライセンスの延長は、以下の手順で簡単に手続きできます。

ライセンスの有効期間が切れた場合
ライセンス期限が切れる数日前から、タスクバーにその旨を知らせるバルーンが表示されます。このバルーンをクリックすると、ダイアログが開くので、ダイアログの説明に従い、簡単に更新をインターネット経由でできます。

保護する台数を増やす
使用中の製品の登録可能ユーザー数をさらに増やしたい場合は、更新時に別製品へと切り替えることができます。この項目をクリックすると手続き用のウェブページが開きますので、そこで詳細をご確認ください。

ソフトウェアの機能

本製品では以下の機能が利用できます（製品により使用できる機能が異なります）：

セキュリティセンター: セキュリティーセンターでは、利用者がマルウェアなどの脅威に素早く簡単に対応できるよう、コンピュータの保護に必要な情報を一目で確認できます。

アンチウイルス: アンチウイルス機能は、お使いのコンピュータをウイルスガードにより常時リアルタイムスキャンを行ったり、指定した方法に従ってコンピュータ全体のスキャンを行い、感染を防ぎます。スキャンにより隔離したファイルの確認や、Windowsを起動せずにマルウェアをスキャンできるブートメディアの作成も、この機能から行えます。

ファイアウォール: ファイアウォールは、外部の不正侵入からコンピュータを防御するため防御する機能で、インターネットやネットワークとコンピュータとの間で送受信されるデータを監視します。許可されていないデータの書き込みやダウンロードを検知すると、ファイアウォールが警告を発し、それらのデータ通信を阻止します。
※この機能はG DATA インターネットセキュリティ、G DATA トータルプロテクションで利用できます。

バックアップ: バックアップは、シンプルかつ簡単な操作で、大切な書類やデータをバックアップする機能です。日常生活は、オンライン音楽サービス、デジタルカメラや電子メールの活用など、ますますデジタル化しており、個人的なデータのバックアップの重要度も増しています。
ハードウェアの故障、過失によるデータ消失、あるいはウイルスやハッカーによるデータ損害に備え、コンピュータに保存されている音楽データ、写真/動画データ、メールデータなどのデータを定期的にバックアップしましょう。
※この機能は G DATA トータルプロテクションで利用できます。

チューナー: チューナーを使用すると、簡単な操作で OS を最適化できます。チューナーは Windows Update の自動確認をはじめ、定期的なデフラグ、レジストリと一時ファイルの定期的なクリーンアップに至るまで、Windows システム内を整理し、処理速度を向上させるツールです。
※この機能は G DATA トータルプロテクションで利用できます。

フィルタリング: フィルタリング機能は、お子様がコンピュータを使用する際などに、ウェブサイトを一定の基準で評価判別して排除したり、コンピュータの利用時間に制限をかける機能です。
※この機能はG DATA インターネットセキュリティ、G DATA トータルプロテクションで利用できます。

データセーフ: データセーフは個人情報等の機密データを保護するための金庫のような機能です。ハードディスクの追加パーティションのような感覚で簡単に利用できます。
※この機能は G DATA トータルプロテクションで利用できます。

オートスタートマネージャー: オートスタートマネージャーは、Windows の起動時に自動起動するプログラムを管理する機能です。通常、それらのプログラムは OS 起動時に読み込まれます。オートスタートマネージャーを使用すると、各プログラムごとに自動起動のタイミングを遅らせたり、起動を防いだり、システムやハードディスクの負荷に応じて設定を調整することができます。この調整により、OS のより高速な起動や、パフォーマンス向上を実現する事が可能となります。

デバイスコントロール: デバイスコントロールは、コンピュータに接続済みのリムーバブルデバイス（例: USBスティック）やCD/DVDドライブやフロッピードライブの利用権限をユーザー単位で管理できる機能です。望ましくないデータのインポート/エクスポートやプログラムのインストールなどを防ぎ、情報漏洩やデータ詐取などの被害を未然に防ぐことができます。
※この機能は G DATA トータルプロテクションで利用できます。

アンチウイルス

この機能を使用して、コンピュータや記録メディアのウイルス感染が無いか、指定した方法でスキャンすることができます。例えば、友人や家族、職場の同僚から借りたUSBメモリや、CD/DVDなどの感染チェック。インターネットからダウンロードしたソフトの感染チェックにも効果を発揮します。

注意: コンピュータや記録メディアのウイルススキャンは追加的な保護機能です。普段はアイドリングスキャンとウイルスガードが常にバックグラウンドで動作しており、マルウェアの脅威に対して最適な保護を維持します。G DATA 製品をインストールする前や、ウイルスガードが無効になっていた間コンピュータにコピーされたウイルスを検出するには、ウイルススキャンを使用してください。

ウイルススキャン

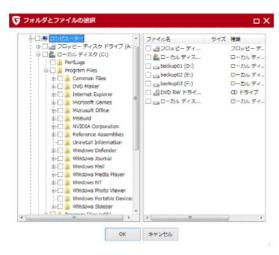
以下の項目からコンピュータやメディアのスキャンを行えます:

コンピュータをスキャン(すべてのローカルドライブ)：ウイルス感染の疑いがある場合など、アイドリングスキャンやスケジュールスキャンとは関係なく、今すぐにコンピュータをスキャンする必要がある時は、ここをクリックします。クリック後は、ただちにスキャンが開始されます。**ウイルススキャンの流れ**の項も参照してください。

メモリとスタートアップをスキャン: 実行中のすべてのプロセスに対して、プログラムファイル および DLL（プログラムライブラリ）をスキャンします。不正プログラムが見つかった場合は、**メモリとスタートアップ領域**から不正プログラムをすぐに除去します。このスキャンは比較的短時間で完了できるため、自動ウイルススキャンなどと一緒

に定期的に実行することをお勧めします。

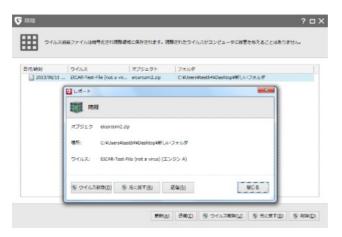
この機能は、データの定期的なウイルススキャンに代わるものではなく、それを補完するものです。

フォルダ/ファイルをスキャン: 選択したドライブ、フォルダ、またはファイルがウイルスに感染していないか調べます。この操作をクリックすると、フォルダとファイルの一覧が表示されます。個々のファイルにターゲットを絞ってスキャンしたり、フォルダ全体のウイルススキャンを行うことができます。
フォルダツリーでは、「+」をクリックするとそのフォルダが展開し、フォルダの内容がファイルビューに表示されます。ウイルススキャンは、チェックボックスにチェックが入っているフォルダまたはファイルに対して、行われます。一部スキャンされないファイルがあるフォルダには、グレーのチェックマークが表示されます。

リムーバブルメディアをスキャン: CD/DVD-ROM、フロッピーディスク、メモリカード、USB メモリなどをスキャンします。この機能を選択すると、コンピュータに接続されているすべてのリムーバブルメディア（トレイに挿入済みのCD/DVD-ROM、メモリカード、または USB経由で接続中の外付けハードディスクやUSB メモリ）をスキャンします。ただし、本製品は書き込み不可のメディアに対してウイルス除去できません。スキャン結果にウイルス検出のログが作成されるだけですので、ご注意ください。

ルートキットをスキャン: ルートキットとは、従来のウイルス検出方法では検出が困難な不正プログラムです。この機能を使うと、ハードディスク内の全データすべてをスキャンすることなく、ターゲットをルートキットに絞ってスキャンします。

隔離されたファイル

ウイルス検出時の処理方法の１つに**隔離**という処理方法があります。この操作を行うと、検出されたファイルが他のファイルに危害を及ぼさないように、コンピュータ上に作成された暗号化領域に保存されます。

隔離領域を表示: このボタンをクリックすると、隔離領域が表示されます。

隔離領域に移動したファイルは、検出された時の状態で保存されます。隔離されているファイルには次の操作が可能です。

- **更新**: 隔離情報を更新します。隔離画面を開いてから時間が経過し、他にもウイルスが検出された場合、それらが表示されます。

- **送信**: 感染ファイルを G DATA に送信します。感染ファイルが新種の不正ファイルである場合は、その後のワクチン開発に活用されます。ユーザーが送信した情報は匿名情報として処理されます。詳細は、マルウェア情報イニシアチブ を参照してください。

  マルウェア情報イニシアチブとは
  G Data セキュリティラボでは、G DATA 製品をご利用のユーザー様を、コンピュータの安全性を脅かす脅威からから保護するため、保護・対策の研究や分析に絶え間なく励んでいます。 マルウェア研究では、マルウェアに関する情報が多ければ多いほど、効果的な保護メカニズムの開発をいち早く進めることができます。これらの情報をG DATAの研究・分析・開発に効率的に取り入れることを可能にするための取り組みが、G DATAマルウェア情報イニシアチブです。 これにより、マルウェアに関するデータをG DATAセキュリティラボに送信することができます。 より多くのユーザー様に参加頂くことで、他のG DATA製品をご利用の方々もインターネットをより安全に利用できるようになります。

- **ウイルス駆除**: 感染ファイルから感染部分のみを駆除し、ファイルを元の場所に戻します。場合によっては、駆除はできない場合もあります。

- **元に戻す**: 隔離ファイルを元に戻します。この処理は例外ケースを除き利用しないでください。利用する場合は、コンピュータのネットワーク／インターネット接続を切断し、未感染データをバックアップするなどした上で、実行してください。

- **削除**: 感染ファイルが不要な場合は、隔離領域から削除できます。

ブートメディア

ブートメディアは、Windows 起動前にスキャンを実行できるブートスキャン機能が搭載しており、本製品のインストール前からコンピュータに感染し、本製品のインストールを妨害する可能性のあるウイルスを駆除するのに役立ちます。詳細は、ブートスキャンの項を参照してください。

ブートメディアを作成する場合は、アンチウイルス画面から**ブートメディアを作成**ボタンをクリックし、ウィザードの指示に従ってください。このウィザードでは、最新の最新のワクチンのダウンロードや、作成メディア種類（CD/DVD/USB）を選択できます。

復元: G DATA トータルプロテクションを使用している場合は、ブートメディアからバックアップイメージをシステムボリュームへ復元、もしくはファイルバックアップを任意のドライブへ復元する事が可能です。復元機能を利用する場合はブートメディアをコンピュータへ挿入し、**G DATA バックアップ（復元）**を選択してください。

オートスタートマネージャー

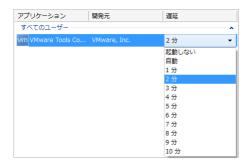
オートスタートマネージャーは、Windows 起動時に自動起動するプログラムを管理するモジュールです。通常、自動起動プログラムは Windows のスタートアップにロードされますが、オートマネージャーを使うと、任意の自動起動プログラムの起動を指定した時間で遅らせて起動でき、Windows の起動を高速化できます。

オートスタートマネージャーを初めて開くと、画面左側にコンピュータにインストール済みの自動起動プログラムの一覧が表示されます。これらは Widows の起動直後に起動されるため、起動所要時間に直接の影響を及ぼします。

自動起動プログラムを遅らせて起動するには、まず対象のプログラムを選択して矢印アイコンをクリックし、右側の領域**スタートアップ（遅延あり）**に移動させます。

遅らせて起動している自動起動プログラムを再び遅延なしで起動するには、対象のプログラムを選択して矢印アイコンをクリックし、左側の領域**スタートアップ（遅延なし）**に移動します。

遅延の設定

オートスタート（遅延あり）のプログラムは、起動を指定した時間で遅らせて起動できます。遅延時間を変更するには、対象プログラムの**遅延カラム**上でクリックします。プルダウン表示されるオプションから、選択してください。

以下のオプションが選択できます。

- **起動しない**: Windows の次回起動時から起動されなくなります。
- **1 - 10 分**: ここで指定する時間に準じてアプリケーションが起動されます。
- **自動**: CPUと保存領域の負荷状況を判断しながら自動起動します。

プロパティ

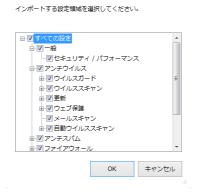
オートスタートマネージャーで表示されるプログラム上でダブルクリックすると、対象の自動起動プログラムのプロパティを表示させることができます。

設定

設定領域では、本製品に搭載されている機能の設定項目を確認したり変更ができます。設定領域の左上アイコンからは、次の機能が利用できます。

設定をエクスポート: 設定ファイルを作成します。複数のコンピュータに製品をインストールして共通の設定でコンピュータを管理する場合、この機能を利用すると便利です。

設定をインポート: ここから設定ファイルをインポートします。インポートを実行するには、ここをクリックし、設定ファイルを指定してインポートを実行します。設定のインポートは、チェックマークを操作して、設定をインポートするモジュールや各モジュールの項目を選択します。

設定をリセット: 何らか理由で現在の設定をデフォルトの状態に戻したい場合は、このアイコンから簡単にリセットできます。リセットは、インポートの操作と同じ様にモジュールやモジュールに含まれる設定項目単位でリセットすることが可能です。

一般

セキュリティ/パフォーマンス

ここでは、コンピュータの性能に応じて簡易的にセキュリティ設定を最適化できます。下のメーターでは、それぞれの設定が及ぼすパフォーマンスやセキュリティ性能への影響を確認できます。まず簡単に動作の調整を行いたい、という場合にはこの機能を使用すると便利です。

- **標準スペックのコンピュータ用 (推奨)**: 2種類のエンジンを使い、最適な保護を提供します。この設定では、ウイルスガード（オンアクセス機能）はすべての読み取り/書き込みアクセスをチェックします。

  エンジン: G DATA には、2種類のエンジンが搭載されています。コンピュータの保護レベルを最適に保つためにも、この設定を利用することをお勧めします。

- **低スペックのコンピュータ用**: 低スペックのコンピュータでは、コンピュータの処理速度が遅くなることがあります。その場合は、1つのエンジンのみを利用することで、パフォーマンス低下を回避することができます。この設定では、ウイルスガード（オンアクセス機能）は実行アクセスのみをチェックします。

  市販の大部分のウイルス対策ソフトには1種類のみのエンジンが搭載されていることからも、1種類のエンジンのみで稼動したとしても、セキュリティ保護レベルが大幅に低下することはありません。

- **ユーザー定義**: エンジンとウイルスガード（オンアクセス機能）の設定をお好みでカスタマイズできます。**モード**では、**無効（非推奨）**以外のオプションを選択してください。**無効（非推奨）**を選択すると、セキュリティレベルが著しく低下するので、推奨されません。

USB キーボードガード

本機能は、USB端末がキーボードになりすましてコンピュータを不正操作する攻撃（BadUSBと呼ばれる脆弱性を悪用する攻撃手法の1つ）からコンピュータを保護します。

機能を有効にすると、新しいUSBキーボードもしくは、キーボードになりすました機器がコンピュータに接続された際にポップアップが表示されます。

接続されたUSB機器が自分の接続したキーボードの場合はポップアップ内の**キーボードを許可**を選択してください。

もし、キーボードではない機器を接続したにも関わらず、このポップアップが表示される場合は、その機器がキーボードになりすましている可能性がありますので、**キーボードをブロック**を選択し、ブロックした機器をコンピュータから取り外してください。

> **注意**:不正操作を防ぐため、ブロックした機器は別のコンピュータにも接続しないでください。

キーボードを許可を選択した後は確認のため認証番号の入力画面が表示されますので、マウスなどで画面に表示された番号を入力してください。入力成功すると接続したキーボードの使用が許可されます。

パスワード

本製品では、設定にパスワード保護を行うことができます。パスワード設定により、別のユーザーが本製品の設定を不正操作することを防ぐことができます。

パスワードを設定するには、設定画面の左側の領域で**パスワード**を選択し、画面右側の**パスワード**と**パスワードの再入力**の2箇所のフィールドで、パスワード入力を行います。**パスワードのヒント**では、万一パスワードを忘れた際に表示するヒントを入力します。
パスワードの設定後に各設定を変更したい場合は、設定画面の右下に表示されるボタンをクリックし、パスワードを入力してください。

メモ: パスワードのヒントは、間違ったパスワードが入力された場合に表示されます。パスワードを設定した本人だけがわかるヒントを指定してください。

メモ: パスワード保護は、セキュリティレベルをアップさせるための有効な手段ですが、1台のコンピュータを複数ユーザーで共同利用する環境では、各ユーザーに専用のアカウントを作成することをお勧めします。これにより、管理者権限を持つユーザーのみが変更することが許可され、制限された権限を持つコンピュータの利用者は変更ができないようになります。

メモ: コンピュータの各ユーザーにユーザーアカウントをセットアップしたなどして、パスワードが不要になった場合は、**パスワードの削除**のボタンからパスワードを削除できます。

注意: パスワードの設定後は、**パスワードの削除**を行わない限り、設定変更を行いたい場合に毎回パスワード入力が必要になりますのでご注意ください。

アンチウイルス

リアルタイム保護

本製品では、リアルタイム保護を継続的に提供するウイルスガード（オンアクセススキャン）機能を提供しています。この機能は、コンピュータ上で行われる読み取り/書き込み処理を常時チェックし、 マルウェアの実行や拡散を未然に防ぎます。ウイルスガードは、アンチウイルス機能で最も重要な機能の1つです。通常は、この機能は無効にしないようにしてください。

リアルタイム保護で利用できる項目です。

- **有効（推奨）**：このチェックマークボックスから、ウイルスガードのオン/オフを切換えできます。
- **エンジンの種類**: ウイルススキャンに使用するエンジンを選択します。G DATAには、2種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現しています。通常は、**2つのエンジン（最高検出力/推奨）**に設定してください。もしコンピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、パフォーマンスを改善することもできます。
- **感染したファイル**: 感染ファイルが検出された場合の処理方法を設定します。デフォルト設定では、感染ファイルの処理方法をユーザーに確認します。なお、データを最高セキュリティで保護するには、**ウイルス駆除（不可能な場合は隔離）**に設定します。
- **感染したアーカイブ**: アーカイブファイル（RAR、ZIP または PST などの拡張子を持つファイル）を通常ファイルと別扱いするかどうかを設定します。なお、隔離されたアーカイブファイルは、元に戻す場合に破損する場合があります。感染したアーカイブは、**ユーザーの操作を待つ**を選択し、検出の度に処理方法をユーザーに選択させることをお勧めします。

- **ふるまい検知**: コンピュータ上のWindows のレジストリやHOSTSファイルへのアクセスやネットワークアクティビティを監視します。これにより、通常のウイルススキャンで検出できなかった不正プログラムを検出します。

- **エクスプロイト対策**: アプリケーションの脆弱性を突くエクスプロイト攻撃により、あなたのPCが不正侵入を受けないように保護します。エクスプロイトからの保護は、アプリケーションを最新の状態に更新する必要があります。G DATA のエクスプロイト対策には、未知の攻撃にも対応できるプロアクティブ技術を搭載しています。

例外

ウイルスガードによるスキャンが不要なドライブ、ファイル、およびフォルダをスキャン対象から除外する設定を行います。

例外を設定するには、以下の手順に沿って行います。

1. **[例外]** を選択します。

2. **ウイルスガード用の例外設定**のダイアログ画面で、**[新規作成]** を選択します。

3. 次の**例外設定**の画面で、除外対象を**ドライブ**、**フォルダ**、**ファイル**を選択できます。

4. ドライブまたはフォルダを指定する場合は、対象を入力欄に直接入力、もしくは、 **[...]** をクリックして対象を指定します。ファイルを指定するには、完全なファイル名もしくはワイルドカードを含むファイル名を設定します。

   メモ: ワイルドカードの機能について

- 疑問符（?）：任意の1文字を表すためのワイルドカード
- アスタリスク（*）：文字列全体を表すためのワイルドカード

例: 拡張子「.sav」のファイルをすべて対象に設定するには、「*.sav」と入力します。連続性のある名前のファイル（text1.doc、text2.doc、text3.doc など）などを保護するには、「text?.doc」と入力します。

この手順を繰り返して例外設定行うことにより、自身の環境に適したウイルスガード用例外をカスタマイズできます。また、作成した例外設定は、**ウイルスガード用の例外設定**画面の**例外**で表示され、編集や削除の操作は、それぞれ **[編集]** と **[削除]** から可能です。

詳細設定

[詳細設定] からは、ウイルスガードによるスキャンの設定確認や変更ができます。

以下の項目を設定できます。

- **モード**: スキャンするタイミングを設定します。設定は、**読み取り/書き込み時にスキャン**、 **読み取り時にスキャン**、もしくは**実行時にスキャン**から選択します。なお、読み取り時にスキャンが行われた場合は、不明なプロセスによる感染があったかどうかを、新規ファイルもしくは新たなファイルバージョンの作成時にスキャンします。その他のケースでは、プログラムが読み取りを行う際にファイルをスキャンします。

- **重要なフォルダを集中的に監視**: このオプションを有効にすると、共有フォルダやコンピュータ上のユーザーデータ、またはクラウドサービス（DropboxやGoogle ドライブ）などを常時、**読み取り/書き込み時にスキャン**するようになります。スキャンのモードに、**実行時にスキャン**以外が設定されている場合、このオプションは灰色で表示されます。

- **ネットワークアクセスのスキャン**: ネットワークアクセスで不正プログラムをスキャンします。自身のコンピュータを、ネットワーク経由でウイルス対策がなされていない第三者のコンピュータと接続する場合には、この機能を有効にしてください。一方、スタンドアロン（ネットワークに未接続）環境、またはネットワーク内の全コンピュータにウイルス対策ソフトがインストールされている環境では、この機能は無効にしておいてください。これらの環境でこの設定を有効のままにしておくと、、重複スキャンが発生することがあり、コンピュータの動作速度の低下につながります。

- **ヒューリスティック**: ワクチンに情報がないウイルス特有の特徴をもつ新種ウイルスを検出します。この検出手法では、保護率を大幅に向上できますが、一方で、未感染ファイルを感染ファイルと判断することもあります。

- **アーカイブのスキャン**: アーカイブ（ZIP、RAR、またはPSTなどの拡張子を持つファイル）をスキャンします。アーカイブのスキャンには、多くの時間を要します。ウイルスガードが常時システムを監視している場合には、アーカイブを解凍する時にアーカイブ内のウイルスを検出するので、この機能は無効にして問題ありません。使用頻度が低い容量の大きなアーカイブのスキャンによるコンピュータの処理速度低下を防止するには、スキャンするアーカイブのサイズを制限します。

- **メールアーカイブのスキャン**: メールアーカイブをスキャンします。なお、本製品では、メールの送受信時にスキャンを実行しているので、通常はこの機能は無効にしていても問題はありません。メールアーカイブのスキャンは、アーカイブのサイズによっては数分間かかることがあります。

- **システム起動時にシステム領域をスキャン**: システム領域のスキャン実行タイミングをシステム起動時に設定します。この設定、もしくは**メディアの交換時にシステム領域をスキャン**のいずれかは常に有効にし、スキャン対象から除外しないでください。

- **メディアの交換時にシステム領域をスキャン**: システム領域のスキャン実行タイミングをメディア（CD/DVDなど）の交換時に設定します。この設定もしくは**システム起動時にシステム領域をスキャン**のいずれかは常に有効にし、スキャン対象から除外しないでください。

- **ダイヤラ/スパイウェア/アドウェア/リスクウェアのスキャン**: ダイヤラ 、スパイウェア、アドウェア、リスクウェアなどの不正プログラムをチェックします。これらの不正プログラムは、望ましくないインターネット接続を勝手に確立したり、ブラウザの閲覧履歴やキーボードへの入力（パスワードなど）を不正に盗みだし、情報漏洩や金銭的な被害に発展する恐れがあります。

- **新しいファイルと変更したファイルのみスキャン**: この機能を有効にすると、以前実行したスキャンにおいて、安全と判断されているファイルで、かつしばらくの間、変更されていないファイルのスキャンをスキップします。スキャンの対象は、新規作成ファイルや変更されたファイルのみがスキャンされるようになり、スキャン速度を大幅に向上できます。

ウイルススキャン

オンデマンドスキャン用のスキャン設定を行います。

リアルタイム保護で利用できる項目です。

- **エンジンの種類**: ウイルススキャンに使用するエンジンを選択します。G DATAには、2種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現しています。通常は、**2つのエンジン（最高検出力/推奨）**に設定してください。もしコンピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、パフォーマンスを改善することもできます。

- **感染したファイル**: 感染ファイルが検出された場合の処理方法を設定します。デフォルト設定では、感染ファイルの処理方法をユーザーに確認します。なお、データを最高セキュリティで保護するには、**ウイルス駆除（不可能な場合は隔離）**に設定します。

- **感染したアーカイブ**: アーカイブファイル（RAR、ZIP または PST などの拡張子を持つファイル）を通常ファイルと別扱いするかどうかを設定します。なお、隔離されたアーカイブファイルは、元に戻す場合に破損する場合があります。感染したアーカイブは、**ユーザーの操作を待つ**を選択し、検出の度に処理方法をユーザーに選択させることをお勧めします。

- **高システム負荷時にはウイルススキャンを停止**: ユーザーがコンピュータ上で作業しない状態になると、スキャンが自動で実行されます。スキャン実行中にコンピュータを使用すると、スキャンは中断されます。中断されたスキャンは、再びコンピュータで作業をしない状態になった場合に再開されます。

例外

ウイルススキャンによるスキャンが不要なドライブ、ファイル、およびフォルダをスキャン対象から除外する設定を行います。

例外を設定するには、以下の手順に沿って行います。

1. **[例外]** を選択します。

2. **ウイルススキャン用の例外設定**のダイアログ画面で、**[新規作成]** を選択します。

3. 次の**例外設定**の画面で、除外対象を**ドライブ**、**フォルダ**、**ファイル拡張子**を選択できます。

4. ドライブまたはフォルダを指定する場合は、対象を入力欄に直接入力するか、もしくは **[...]** をクリックして対象を指定します。拡張子を指定するには、拡張子を入力して **[OK]** を選択します。（例: 拡張子「iso」を持つファイルを例外設定するには、「.iso」もしくは「iso」と入力）

この手順を繰り返して例外設定行うことにより、自身の環境に適したウイルススキャンをカスタマイズできます。作成した例外設定は、**ウイルススキャン用の例外設定**画面の**例外**で表示され、編集や削除の操作は、それぞれ **[編集]** と **[削除]** から可能です。

アイドリングスキャンでも例外を有効にする: アイドリングスキャンは、ユーザーがコンピュータを利用しない時に自動的に起動するスキャン機能です。アイドリングスキャン中に、ユーザーが再び作業をはじめると、実行中のスキャンは中断されます。ユーザーはスキャンによるコンピュータ速度の低下に悩まされることはありません。ここではアイドリングスキャンでスキャン対象から除外するファイルやフォルダを指定します。

詳細設定

[詳細設定] からは、**ウイルススキャン**によるスキャンの詳細内容を確認したり、変更したりできます。

以下の項目を設定できます。

- **ファイルの種類**: ウイルススキャンの対象になるファイルの種類を指定します。**プログラムファイルとドキュメントのみ**を選択すると、速度優先でウイルススキャンします。

- **ヒューリスティック**: ウイルスデータベースに情報がないウイルス特有の特徴をもつ新種ウイルスを検出します。この検出手法では、保護率を大幅に向上できますが、一方で、未感染ファイルを感染ファイルと判断してしまう誤検出のケースもあります。

- **アーカイブのスキャン**: アーカイブ（ZIP、RAR、またはPSTなどの拡張子を持つファイル）をスキャンします。アーカイブのスキャンには、多くの時間を要します。ウイルスガードが常時システムを監視している場合には、アーカイブを解凍する時にアーカイブ内のウイルスを検出するので、この機能は無効にしておいてください。使用頻度が低い容量の大きなアーカイブのスキャンによるコンピュータの処理速度低下を防止するには、スキャンするアーカイブのサイズを制限します。

- **メールアーカイブのスキャン**: メールアーカイブをスキャンします。

- **システム領域のスキャン**: システム領域をスキャンします。この設定は常に有効にしておいてください。

- **ダイヤラ/スパイウェア/アドウェア/リスクウェアのスキャン**: ダイヤラ 、スパイウェア、アドウェア、リスクウェアなどの不正プログラムをチェックします。これらの不正プログラムは、望ましくないインターネット接続を勝手に確立したり、ブラウザの閲覧履歴やキーボードへの入力（パスワードなど）を不正に盗みだし、情報漏洩や金銭的な被害に発展する恐れがあります。

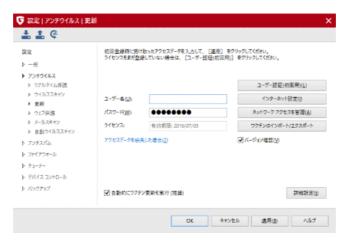
- **ルートキットのスキャン**: 従来型のウイルス対策ソフトによる検出方法では検出が困難なルートキットをスキャンできます。

- **新しいファイルと変更したファイルのみスキャン**: この機能を有効にすると、以前スキャンしたことがあり、その際に安全と判断されたファイルのスキャンを省略します。スキャンの対象は、新規作成ファイルや変更されたファイルのみがスキャンされるようになり、スキャン速度を向上させることができます。

- **ログの作成**: ウイルススキャンのログを記録します。ログを閲覧するには、起動画面の右上のログアイコンをクリックします。

- **リムーバブルメディアをスキャン**: このチェックボックスを有効にすると、リムーバブルメディア（例: USBメモリ、USB外付けハードディスクなど）がコンピュータに接続された際に、ウイルススキャンを実行するかを確認するメッセージボックスが表示されます。

更新

ワクチンやプログラム更新が機能しない場合には、この領域で設定を確認してください。更新を利用するには、有効な**アクセスデータ（ユーザー名とパスワード）**が入力されている必要があります。アクセスデータは、製品の初回認証時に登録先メールアドレスに送信されています。

初めて認証を行う場合は、[ユーザー認証（初回用）] を選択します。 インターネット設定では、プロキシサーバーや更新ファイル用のサーバーを指定できます。

> **更新ネットワークを管理**: ワクチンやソフトウェアアップデートのダウンロードを許可するネットワークを選択できる機能です。Wi-Fiやモバイルネットワークでインターネットに接続している環境でワクチンやプログラム更新を行うと、そのネットワークでのダウンロードを許可するかどうか選択するダイアログが表示されます。そこで選択した設定を、この機能で後から変更することができます。
> 例えば、外出時にモバイルネットワークを使用中に大量のデータ通信を行いたくない場合、そのネットワークをブロック登録するのがお勧めです。

ワクチンのインポート/エクスポート（オフライン更新用）: インターネット接続に制約がある環境用のワクチンをインポート/エクスポートする機能です。ワクチンのエクスポートは、インターネットでG DATAのライセンス登録を行ったコンピュータ上でのみ可能です。オフライン更新を利用する場合は、セキュリティの観点から、できるだけ頻繁に更新することをお勧めします。

設定画面でインポートかエクスポートを選択し、ワクチン保存先フォルダを選択した後でワクチン更新を行うと、指定したフォルダ内にワクチンデータが保存される、もしくは、フォルダ内からワクチンデータが読み込まれます。ワクチンデータをエクスポートする際、使用中のワクチンがすでに最新の場合はエクスポートされませんのでご注意ください。

バージョンチェック: ワクチンファイルの差分更新を実行するかについて、設定できます。エンジンの破損や誤ってワクチンファイルを削除した場合以外は、通常、この設定は有効にしておいてください。

自動的にワクチン更新を実行: デフォルト設定の自動更新を利用しない場合にチェックを外します。なお、ワクチンが長期間更新されないと、コンピュータの保護レベルが著しく低下します。この設定は、特殊なケースを除き無効化しないでください。もし更新間隔が短すぎる場合は、必要に応じて実行頻度を調節してください。
実行頻度内の、毎日（インターネット接続時）、もしくは毎時（インターネット接続時）という設定は、コンピュータがインターネット接続中かどうかを判断し、インターネットに接続している場合のみ更新処理を行う設定です。これはコンピュータを外へ持ち出している場合などに適した設定で、不必要な処理を減らす事ができます。

ログを作成: ワクチン更新やウイルス検出などをログとして記録します。起動画面の右上にあるログアイコンをクリックすると、ログを閲覧できます。

ユーザー認証（初回用）

ユーザー認証が完了していない場合は、ここから**レジストレーション番号**を入力して認証を行うことができます。ボックス製品を購入された場合は、レジストレーション番号はユーザー登録用紙に記載されています。ダウンロード版を購入された場合は、メールで送信されています。

製品を認証するには、**[ユーザー認証（初回用）]** をクリックすると現れる画面に、**レジストレーション番号、姓、名、メールアドレス（PC用）**を入力し、**[登録]** をクリックします。認証が正常に行われると、**「登録に成功しました。アクセスデータは自動的に本製品に登録され、メールでもアクセスデータが送信されます。」**というメッセージが表示されます。**[OK]** をクリックして、この画面を閉じます。

注意: アクセスデータは、ここで登録したメールアドレスに送信されます。メールアドレス入力の際は、誤入力のないようにご注意ください。アクセスデータは、再インストールまたは2台目以降のPCを認証する際（複数台版を購入の場合）に必要です。

認証後は、ユーザー名とパスワードの入力欄に生成されたアクセスデータが自動的に入力されます。これで更新を実行できるようになります。

認証に失敗する場合

まず、ブラウザを使ってインターネットに正常に接続されているか確認してください。ブラウザでインターネット閲覧できるにもかかわらず更新できない場合は、プロキシサーバーに問題がある可能性があります。この場合は、インターネット設定 を選択して、プロキシサーバーに入力されている情報を確認してください。

インターネット設定

プロキシサーバー を使用する環境では、**プロキシサーバーを使用**にチェックを入れてください。この設定は、インターネット更新が正常に機能しない場合にのみ変更します。プロキシサーバーの入力欄で入力する情報については、システム管理者またはインターネット接続プロバイダに確認してください。アクセスデータは必要に応じて入力してください。

プロキシサーバー: プロキシサーバーは、ネットワーク内のPCからのリクエストを束ねてインターネットに接続します。社内ネットワークなどにプロキシサーバーが導入されている場合は、**プロキシサーバーを使用**にチェックを入れ、必要な情報を入力することで、更新が利用にできるようになります。

ウェブ保護

ウェブ保護を有効にすると、ウェブ閲覧中もコンピュータをマルウェアから保護することができます。ウェブ保護では次の設定が可能です。

- **インターネットコンテンツ（HTTP）のスキャン**: インターネット閲覧するだけで感染する危険がある、ウェブページ経由のウイルスをスキャンします。ユーザーが閲覧しようとしたコンテンツで不正プログラムを検出すると、そのコンテンツの実行をストップして、コンピュータを感染から守ります。なお、ウイルスが検出された場合、ウェブページは表示されません。この設定を有効にするには、**インターネットコンテンツ（HTTP）のスキャン**にチェックを入れます。

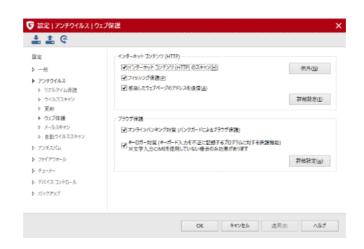
ウェブコンテンツのスキャンを無効にした場合は、ウイルスガードは必ず有効にしてください。不正プログラムの実行時に、ウイルスガードがこれを検出します。

特定サイトを例外に設定するには、例外の項を参照してください。 [詳細設定] からは、インターネットコンテンツ関連の設定を行うことができます。

- **フィッシング保護:** オンラインバンキング、オンラインショップ、ネットオークションの偽サイトに誘導し、顧客データやログイン情報を盗むフィッシングサイトやその他の詐欺、悪質サイトをブロックします。インターネットを閲覧する時は、常時有効化することをお勧めします。

- **感染したウェブページのアドレスを送信**: 危険と判断されたウェブページの情報を G DATA へ自動送信します。なお、このアドレスの送信は、匿名で処理されます。送信元が特定できるデータは送信されません。収集データは、ユーザーがインターネットをより安全に利用できるために役立てられます。

- **オンラインバンキング対策**: G DATA のオンラインバンキング対策機能バンクガードは、ネットバンキングを標的とするバンキング系トロイの木馬による中間者攻撃（man-in-the-middle攻撃）を検出し、リアルタイムで保護します。バンキング系トロイの木馬は、金銭的被害をもたらす悪質な不正プログラムで、現在、世界各国で猛威を振るっています。銀行サイトがオンライン取引の暗号化をしていても、攻撃は復号化されたブラウザ上で行われるため、通常のウイルス対策ソフトでは攻撃の回避が困難でした。G DATA では、ネットワークライブラリをリアルタイムでチェックすることにより、man-in-the-middle攻撃によるブラウザの不正操作を保護します。

- **キーロガー対策**: コンピュータで入力したキー入力を不正に記録するプログラムを監視します。この機能は常時有効にしておく事をお勧めします。
  ※キーロガー対策は、文字入力にIMEを使用していない場合のみ効果があります。
  IMEを使用しない文字入力を行うには、「テキストサービスと入力言語」（Windowsの言語バーを右クリックして設定を選択することで開くことができます）を開き、「全般」画面で追加ボタンをクリックし英語（米国）などの英語入力を選択、適用して文字言語を追加します。
  その後、言語バーの言語設定をJPからENに変更する事でIMEを使用しない文字入力が行えるようになります。

例外

ウェブサイトを例外として設定するには、次の手順に沿って行います。

1 **[例外]** をクリックします。そうすると、**ウェブ保護用の例外設定**の画面が開きます。この画面では、ユーザーが安全なサイトとして登録したページが表示されます。

2 例外のウェブサイトを **ウェブ保護用例外**に追加するには、**[新規作成]** をクリックします。入力画面が開くので、URL の欄にウェブページのアドレス（例： www.gdata.co.jp）と、必要に応じて**説明**の欄に登録の理由などを入力します。

3 [OK] をクリックすると、ウェブページが例外サイトとして追加され、ウェブ保護の対象から除外されます。

例外に登録したウェブページの編集や編集は、登録した項目を選択し、編集の場合は **[編集]** を、削除の場合は **[削除]** をクリックします。

詳細設定

ウェブ保護が監視するサーバーポート番号を設定します。デフォルト設定では、通常のインターネット閲覧に使用する 80 が設定されています。

- **ブラウザのタイムアウトを防止: インターネットコンテンツ（HTTP）のスキャン**にチェックを入れた場合、ウェブコンテンツをブラウザに表示する前に不正ルーチンのチェックが行われます。この処理はデータ量によっては処理時間がかかり、ブラウザが表示データをすぐに受信できないため、エラーメッセージが表示されることがあります。**ブラウザのタイムアウトを防止**にチェックを入れると、このエラーメッセージが表示されず、コンテンツ全体のチェックが終了するとウェブページが通常どおり表示されるように

なります。

- **ダウンロードの容量制限**: 指定したサイズを超過したダウンロードファイルでの**インターネットコンテンツ（HTTP）のスキャン**を解除します。この容量制限を利用することで、**インターネットコンテンツ（HTTP）のスキャン**によるインターネットの通信速度低下を回避できるます。なお、容量制限した場合は、ウイルスガードは必ず有効にしておいてください。

メールスキャン

メールスキャンは、送受信メールや添付ファイルでウイルススキャンする機能です。メールスキャンで検出した添付ファイルは、削除や修復の操作ができます。

メモ: Microsoft Outlook には、専用プラグインがインストールされます。このプラ

グインは、Outlook 上でより簡単なウイルスチェックを実現するツールです。メールスキャンで設定できる POP3/IMAP ベースの保護と全く同じ機能を提供します。メールまたはフォルダのスキャンを実行するには、Outlook メニューバーの **[ツール] > [フォルダのウイルスをスキャン]** を選択します。

受信メール

受信メールでは、次の設定が可能です。

- **感染した場合**: 感染メールが検出された場合の処理方法を設定します。コンピュータ環境に応じて、最適な設定を選択してください。通常は、**ウイルス駆除（不可能な場合は添付ファイル / メール本文を削除）**の使用をお勧めします。

- **受信メールのスキャン**: インターネット接続中の全受信メール に対して、ウイルススキャンを実行します。

- **感染メールへのレポート添付**: ウイルスが検出された場合、感染メールの件名欄に**「ウイルス」**という警告を挿入します。また、メール本文の先頭に**「注意！このメールはウイルスに感染しています」**というメッセージ、ウイルスの名称、ウイルスの駆除または感染ファイルを修復したなどの情報を表示します。

送信メール

送信メールでは、次の設定が可能です。

- **送信前のメールスキャン**: ウイルス添付メールの外部送信を防ぐために、送信前にチェックします。この機能が有効な場合に、ウイルス添付メールを送信しようとすると、**「メール [件名] には次のウイルスがあります: [ウイルス名]」**というメッセージが表示され、メールの送信はブロックされます。

スキャンオプション

スキャンオプションでは、基本的なウイルススキャンの基本的な設定を行います。次の設定が可能です。

- **エンジンの種類**: ウイルススキャンに使用するエンジンを選択します。G DATAには、2種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現しています。通常は、**2つのエンジン（最高検出力/推奨）**に設定してください。もしコンピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、パフォーマンスを改善することもできます。

- **アウトブレイクシールド**: パンデミック型のウイルス感染メールを常時監視してブロックするクラウド型機能、アウトブレイクシールド （OutbreakShield）を有効/無効を設定します。アウトブレイクシールドを有効にすると、受信メールにチェックサムが作成され、クラウド上のアンチスパムブラックリストと照会が行われます。これにより、ワクチンに

依存することなく、ウイルスが最初に発見された時点から数十秒から数分内でウイルスメールとして検出できます。

詳細設定

メールプログラムに**標準ポート**を割り当てていない場合には、メールの送受信に使用する**ポート**を**サーバーポート番号**の欄に入力してください。**[標準]** をクリックすると、自動的に標準のポート番号にリセットされます。複数のポートをスキャンさせたい場合は、コンマ（ , ）でそれぞれのポート番号を区切って入力してください。

> メモ: Microsoft Outlook には、専用プラグインがインストールされます。このプラグインは、Outlook 上でより簡単なウイルスチェックを実現するツールです。Outlook プラグインを使うと、**Outlook** 上で簡単な操作でメールスキャンができるようになります。スキャンを実行するには、スキャンする対象のメールまたはフォルダを選択し、G DATA アイコンをクリックして実行する操作を選択します。

G DATA のメールスキャンは、メールプログラムが実際にメールを受信する以前に処理を行うため、大量のメールを受信する場合やインターネット回線速度が遅い環境では、メールプログラムがタイムアウトのエラーメッセージを表示することがあります。この原因は、メールスキャンによるスキャンで、メールプログラム側でのメール受信で遅延が発生するためです。**メールクライアントのタイムアウトを防止**にチェックを入れると、タイムアウトエラーが表示されなくなります。受信メールは、スキャン完了次第、メールプログラムに引き渡されます。

自動ウイルススキャン

ユーザーがコンピュータを使用していない時にスキャンが自動実行されるアイドリングスキャン機能やスキャン対象、スキャン実行日時や頻度、エンジンの種類などをカスタムしたスケジュールスキャンを設定できます。

ウイルススキャンのスケジュール設定で、**[新規作成]** をクリックします。ダイアログ画面が開くのでまず名前を入力し、必要な項目を設定してください。例えば、ダウンロードしたファイルを毎日特定の時間にスキャンする場合は、**スキャン範囲**の**次のフォルダとファイルをスキャン**を選択し、**[選択]** ボタンから対象フォルダを選択します。次に**スケジュール**の**実行頻度**で**毎日**を選択、そして時間を設定して、**[OK]** をクリックすれば設定は完了です。

一般

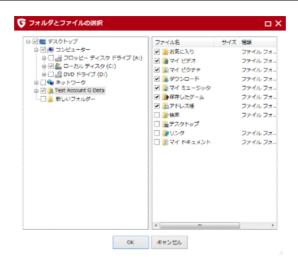
新規作成する自動ウイルススキャンジョブに名前をつけます。ジョブにはわかりやすい名前をつけてください。

スキャン終了後にコンピュータの電源を切る（ユーザーがログインしていない場合）にチェックを入れると、スキャン後にコンピュータを自動的にシャットダウンします。

ジョブ: 実行されるウイルススキャン処理の単位を**ジョブ**と呼びます。

スキャン範囲

ウイルススキャンを実行する対象を設定します。スキャンの対象は、**ローカルのハードディスクドライブ、メモリとスタートアップ、次のフォルダとファイルをスキャン**から選択できます。次のフォルダとファイルをスキャンを選択した場合は、**[選択]** をクリックすると対象を指定します。

フォルダとファイルの選択: フォルダのツリー構造で「+」をクリックするとそのフォルダが展開し、フォルダの内容がファイルビューに表示されます。チェックが入っているフォルダまたはファイルがスキャンの対象になります。なお、フォルダ内ですべてのファイルがマークされるとチェックマークは黒で表示されます。一部のファイルが選択されていないフォルダは、グレーのチェックマークで表示されます。

スケジュール

ジョブを実行するタイミングを設定します。実行のタイミングは、**実行頻度**と**時間**を組み合わせて設定します。**実行頻度**で**システム起動時**を選択した場合は、**時間**は非表示となります。

- **スケジュール実行後にコンピュータの電源が切れていた場合、次回の起動時にジョブを実行**: コンピュータを起動していなかったため実行できなかったスキャンジョブを、コンピュータの次回起動した時に自動的に実行します。

- **バッテリモードでは実行しない**: ノートパソコン用の設定です。バッテリー駆動時はスキャンジョブを実行せずに、AC電源での駆動時にスキャンジョブを実行します。

スキャン設定

自動ウイルススキャン用のスキャン設定について定義します。

- **エンジンの種類**: ウイルススキャンに使用するエンジンを選択します。G DATAには、2種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現しています。通常は、**2つのエンジン（最高検出力/推奨）**に設定してください。もしコンピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、パフォーマンスを改善することもできます。

- **感染したファイル**: 感染ファイルが検出された場合の処理方法を設定します。デフォルト設定では、ウイルスが検出されるとウイルスと感染ファイルについてのログが残されます。最高セキュリティで保護するには、**ウイルス駆除（不可能な場合は隔離）**に設定します。

- **感染したアーカイブ**: アーカイブファイル（RAR、ZIP または PST などの拡張子を持つファイル）を通常ファイルと別扱いするかどうかを設定します。なお、アーカイブファイルを隔離すると、元に戻す場合にファイルが破損する場合があります。感染したアーカイブは、**ログを残すのみ**を選択し、検出の度に処理方法をユーザーが選択することをお勧めします。

- **高システム負荷時にはウイルススキャンを停止**: ユーザーがコンピュータ上で作業しない状態になると、スキャンが自動で実行されます。スキャン実行中にコンピュータを使用すると、スキャンは中断されます。中断されたスキャンは、再びコンピュータで作業をしない状態になった場合に再開されます。

[詳細設定] からはスキャン詳細設定の編集や確認ができます。

次の設定が可能です。

- **ファイルの種類**: スキャン対象とするファイルの種類を選択します。
- **ヒューリスティック**: ウイルスデータベースに情報がないウイルス特有の特徴をもつ新種ウイルスを検出します。この検出手法では、保護率を大幅に向上できますが、一方で、未感染ファイルを感染ファイルと判断してしまう誤検出のケースもあります。
- **アーカイブのスキャン**: アーカイブ（ZIP、RAR、またはPSTなどの拡張子を持つファイル）をスキャンします。アーカイブのスキャンには、多くの時間を要します。ウイルスガードが常時システムを監視している場合には、アーカイブを解凍する時にアーカイブ内のウイルスを検出するので、この機能は無効にしておいてください。使用頻度が低い容量の大きなアーカイブのスキャンによるコンピュータの処理速度低下を防止するには、スキャンするアーカイブのサイズを制限します。
- **メールアーカイブのスキャン**: メールアーカイブをスキャンします。
- **システム領域のスキャン**: システム領域をスキャンします。この設定は常に有効にしておいてください。
- **ダイヤラ/スパイウェア/アドウェア/リスクウェアのスキャン**: ダイヤラ 、スパイウェア、アドウェア、リスクウェアなどの不正プログラムをチェックします。これらの不正プログラムは、望ましくないインターネット接続を勝手に確立したり、ブラウザの閲覧履歴やキーボードへの入力（パスワードなど）を不正に盗みだし、情報漏洩や金銭的な被害に発展する恐れがあります。
- **ルートキットのスキャン**: 従来型のウイルス対策ソフトによる検出方法では検出が困難なルートキットをスキャンできます。
- **ログの作成**: ウイルススキャンのログを記録します。ログを閲覧するには、起動画面の右上のログアイコンをクリックします。

ユーザーアカウント

コンピュータがネットワークに接続されている環境で、接続先もスキャン対象とする場合は、接続先へのアクセス権が必要となります。アクセスに必要な**ユーザー名**、**パスワード**、**ドメイン**を入力してください。

ログ

本製品に搭載されている各機能には、保護などを行った際の動作を記録、確認するためのログ機能が搭載されています。

アンチウイルスのログ

アンチウイルスを選択した状態でログアイコンを選択すると、ウイルスからの保護状況や、ワクチンのアップデート状況が記録されます。

列見出しの **開始時刻**、**種類**、**内容** もしくは**ステータス**をクリックすると、ログを並び替えることができます。［**名前を付けて保存**］では、ログをテキストファイルに保存し、［**印刷**］ではログを印刷できます。ログを削除するには、対象を選択してから、［**削除**］ボタン（もしくはキーボードの Delete キー）を押してください。

FAQ: ブートスキャン

本製品には、Windows 起動前にスキャンを実行できる**ブートスキャン**機能が搭載されています。 ブートスキャンは、本製品をインストールする前からコンピュータに感染し、本製品のインストールを妨害する可能性のあるウイルスの駆除をするのに役立ちます。

ブートとは: コンピュータの電源を入れると、通常は自動的に Windows OS が起動します。このプロセスを「ブート」と呼びます。このプロセスでは Windows OS だけでなく代わりに別のOSを自動的に起動させることもできます。本製品のブートメディアを使用すると、ブートの際、 Windows の代わりに専用OSでコンピュータを起動することができ、そのOS上でウイルススキャンを行う事ができます。

ブートスキャンの準備

ブートスキャンは、本製品をインストールする前からコンピュータに感染し、本製品のインストールを妨害する可能性のあるウイルスの駆除をするのに役立ちます。このブートスキャン機能は、Windows を使用せずにコンピュータをブートメディアから起動してスキャンを行う機能です。

CD/DVD からのブート: コンピュータが、ブートCD/DVD から起動できない場合は、以下の手順をお試しください。
（この作業は、コンピュータの操作に慣れた上級者が設定されることをお勧めします）

1 コンピュータをシャットダウンします。

2 コンピュータを起動し、**BIOS 設定画面**を表示します。通常 BIOS 設定を行うには、コンピュータの起動（= ブート）時に **Delete** キーを押します。

BIOS 設定画面が Delete キーで表示されない場合: コンピュータのメーカーによっては、**F2 キー**、**F10 キー**、または**その他のキー**が割り当てられている場合もあります。コンピュータの取扱説明書もしくはホームページなどでご確認ください。

3 次に、BIOS 設定画面で、ブートデバイスの優先順位を変更します。BIOS の各設定項目をどのように変更するかはコンピュータによって異なりますので、コンピュータの取扱説明書をお読みください。変更後のブート順は **CD/DVD: , C:** にします。具体的には、CD/DVD ドライブを [1st Boot Device] （第1ブートデバイス）とし、Windows OS がインストールされているハードディスクパーティションを [2nd Boot Device] （第2ブートデバイス）とします。

4 変更を保存して、コンピュータを再起動します。これでブートメディアからブートできる状態になりました。

ブートスキャンを中断するには: 通常、コンピュータに起動中にブートメディアが挿入されているとブートスキャンの画面が表示されます。Windows 起動画面を表示したい

場合は、ブートスキャンのメニュー画面で矢印キーを使い、**Microsoft Windows** を選択し、**Enter** キーを押します。すると、Windows が通常通り起動します。

USBメモリからのブート: USBメモリのブートメディアからブートする場合も、CD/DVDと同じ要領で 1st Boot Device として認識されるように設定してください。それでも起動時に認識されない場合は、コンピュータの起動時に**ブートメニュー**を使用し、対象のUSBメモリを選択して、ブートを行ってください。

ブートスキャンの流れ

ブートスキャンを実行するには、以下の手順に沿って行ってください:

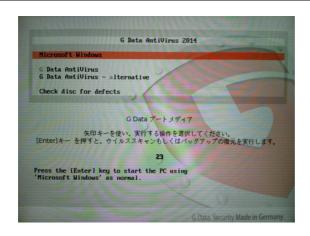
1 **CD版製品でのブートスキャン**: **製品CD/DVD** をCD/DVDドライブに挿入します。表示された起動ウインドウで、**［キャンセル］** をクリックし、コンピュータをシャットダウンします。

ダウンロード版製品でのブートスキャン: G DATA を起動し、**ウイルス対策**タブを選択します。次に、右下の**［ブートメディアを作成］** を選択して、ブートメディア を作成します。作成が完了したら、作成したブートメディアをコンピュータに挿入して、コンピュータをシャットダウンします。
※ブートメディアを挿入後に起動画面が表示された場合は、**［キャンセル］**をクリックしてコンピュータをシャットダウンします。

メモ: Windows XP 上では、ブートメディア作成時に**「IMAPI 2.x がインストールされていません」**というメッセージが表示されることがあります。これは、古いOSでデータをメディアにコピーするために必要な Microsoft の更新プログラムです。Microsoft のサイトからダウンロードしてインストールしてください。

USBメモリを利用したブートスキャン: G DATA を起動し、**ウイルス対策**タブを選択します。次に、右下の**［ブートメディアを作成］**を選択して、ブートUSB を作成します。作成が完了したら、作成したブートUSB をPCに差し込み、コンピュータをシャットダウンします。
※ブートUSBの挿入後に起動画面が表示された場合は、**［キャンセル］**をクリックしてコンピュータをシャットダウンします。

注意: ブートUSBから起動する場合は、コンピュータがUSBメモリからブートできる状態でなければなりません。多くの場合は、起動時にコンピュータのブートメニューを使用する事でブート可能です。詳しい解説は、ブートスキャンの準備の項の**USBメモリからのブート**を確認ください。

2 コンピュータを再起動します。**G DATA ブートスキャン**のスタートメニューが表示されます。

3 矢印キーで G Data AntiVirus(もしくはG Data AntiVirus + Backup） を選択し、Enter キーで確定してください。自動的に Linux OS が起動し、ブートスキャン用画面が表示されます。

メモ: プログラム画面が正常に表示されない場合には、コンピュータを再起動して G Data AntiVirus - Alternative（もしくはG Data AntiVirus + Backup - Alternative） を選択してください。

メモ: トータルプロテクション を使用している場合、この画面の後にダッシュボード画面が表示されます。**AntiVirus を起動**もしくは**復元を開始**を選択してください。

4 ワクチン更新を実行するよう促されます。

5 ［はい］をクリックし、次の画面で［スタート］ボタンを押すと更新が始まります。ワクチンデータが更新されると、「**更新できました**」というメッセージが表示されます。

メモ: 自動インターネット更新機能は、IP アドレスを自動割当機能（DHCP）を持つルータを使用している場合にのみ、利用できます。インターネット更新が利用できなくても、古いワクチンを利用して、ブートスキャンを実行できます。ただし、この場合には、本製品のインストール後できるだけ早いうちに、更新したワクチンを使って、ブートスキャンを実行してください。

6 スキャンのタブを選択して、スキャン領域に移動します。［**コンピュータ**］をクリックすると、コンピュータ全体のスキャンが開始されます。一般的に、コンピュータ全体のスキャンを行った場合は、スキャン終了まで数時間以上の時間を要します。一部のフォルダのみのスキャンで十分な場合は、［**ファイルとフォルダ**］を押して、対象のフォルダを選択してスキャンすると、スキャン時間も短く済み、効率的です。

7 **ウイルスが検出されたら**、本製品が提案する処理方法から適当なものを選択して、ウイルス駆除を行ってください。ウイルスを駆除できたら、オリジナルファイルが再び使用可能な状態になります。 なお、ファイルがシステムファイルや重要なファイルと思われる場合は、削除しないことをお勧めします。

メモ: 削除を選択する場合は、対象のファイルが削除されてもシステムに問題を引起さないことを確かめてから、操作を実行してください。

8 ウイルススキャンが完了したら、画面右上の X マークをクリックします。ダッシュボード画面が表示されるので、［**終了**］をクリックし、**再起動**または**シャットダウン**を選択します。

9 ドライブのトレイが開いたら、**ブートCD** を取り出します。（**USBメモリ** を使用してブートスキャンしている場合は、コンピュータのUSBスロットに差し込まれているUSBメモリを抜きます。）

10 コンピュータを再起動し、通常通り Windows OS を起動します。（CDやUSBメモリが挿入されている場合は、すぐに取り出してください）

FAQ: 各種機能について

G DATA アイコン

本製品の保護機能が有効に機能しているかどうかは、タスクバー上の G DATA アイコンで確認できます。

このアイコンが表示されている時は、G DATA によるセキュリティ保護が有効で、コンピュータが適切に保護されていることを意味しています。

警告マーク付きのアイコンが表示される時には、セキュリティ保護が有効になっていないことを意味しています。このアイコンは、ウイルスガードを無効にしたり、セキュリティ保護に問題がある場合に表示されます。

このアイコンが表示されている時は、本製品がインターネットから更新ファイルをダウンロードしています。

G DATA アイコン上で右クリックをすると、右クリックメニューが表示されます。右クリックメニューからは、ユーザーがよく使用する操作が選択できます。

画像はトータルプロテクションのものです。

ここでは以下の操作を選択できます:

- **G DATA（製品名）を起動**: 本製品プログラムのセキュリティセンターを呼び出します。セキュリティセンターに関する詳細は、セキュリティセンターを参照してください。
- **ウイルスガードを無効にする**: ウイルスガードの有効／無効を切り替えます。大容量のファイルをコピーしたりする際にウイルスガードを無効にすると処理がより高速に行われますが、ウイルスガードを無効にする期間は最小限に抑えてください。またウイルスガードが無効な間は、インターネットやスキャン未実行のメディア（CD/DVDやUSBメモリなど）と接続しないようにしてください。

- **ファイアウォールを無効にする**: ファイアウォールが搭載されている製品では、右クリックメニューからファイアウォールの有効／無効を切り替えることができます。インターネット接続環境では、ファイアウォールを無効にした後も、コンピュータは引き続きインターネットに接続されます。このとき外部からの攻撃から保護されませんので、ファイアウォールを無効にする際は注意してください。

- **オートパイロットを無効にする**: ファイアウォールのオートパイロット機能の有効／無効を切り替えます。オートパイロットはファイアウォールの処理をユーザーに代わって自動的に判断する機能で、これを無効にすると、ネットワーク接続についてユーザーへ確認が行われるようになります。通常はオートパイロットを有効にした状態で利用することをお勧めします。

- **ワクチンを更新**: 今すぐにワクチン更新を手動実行します。コンピュータの適切な保護には、ワクチン更新は非常に重要です。ワクチン更新は通常、自動更新に設定しておいてください。インターネット更新に関する詳細は、更新の項を参照してください。

- **データセーフを開く**: トータルプロテクションを使用している場合は、データセーフ作成後にここから任意のデータセーフを開く事ができます。

- **統計情報**: メール、ウェブ、ウイルスガードなどのスキャン統計を確認できます。

ウイルススキャンの流れ

ウイルススキャンは、コンピュータ上のマルウェアをスキャンする機能です。ウイルススキャン中にウイルスが検出されると、検出されたウイルスへの対処方法を選択できます。

検出されたウイルスには、それぞれの検出ごとに、削除、駆除、隔離といった対処が可能です。

1. ウイルススキャンを開始します。ウイルススキャンの開始方法は、アンチウイルスの各項目を参照してください。

2. コンピュータ上でスキャンが始まると、スキャンのステータス情報を表示する画面が開きます。

   画面上部のステータス表示バーには、スキャンの進捗状況が表示されます。ウイルススキャンのプロセスに関する設定は、スキャン中に行うことができます。設定できる項目は次の通りです。

   - **システム負荷が高い時はウイルススキャンを停止**: ユーザーがコンピュータで作業を行っている間は、ウイルススキャンを自動的に停止します。

- **スキャン終了後にコンピュータの電源を切る**: ウイルススキャン終了後に、コンピュータが自動的にシャットダウンします。例えば、一日の作業終了時にスキャンを行う場合などに使用すると便利です。

- **パスワード保護されたアーカイブ**: アーカイブがパスワードで保護されている場合、このアーカイブはスキャンされません。ここにチェックを入れると、スキャンできなかったパスワード保護されたアーカイブを表示します。これらのアーカイブにウイルスが潜んでいたとしていても、解凍しない限り、ウイルスがシステムに感染する可能性はありません。

- **アクセス拒否されたファイル**: Windowsでは、通常、アプリケーションが自身の動作のために使用するファイルを、そのアプリケーションの実行中にスキャンできません。スキャン実行中は、可能な限り、他のプログラムを実行しないようにしてください。ここにチェックを入れると、スキャンできなかったデータが表示されます。

3a

ウイルススキャン結果が画面に表示されます。ウイルスが検出されなければ、**［閉じる］**をクリックして画面を閉じます。

3b

ウイルスが検出された場合は、**［操作の実行］**をクリックして感染ファイルの処理を行います。

デフォルト設定（設定 | アンチウイルス | ウイルススキャンで、何も変更しなかった場合）では、感染ファイルからウイルスを駆除します。ウイルスを駆除に成功したファイルは再び普通に使用してもコンピュータに支障をきたしません。

駆除できない場合には、ファイルは隔離領域に移動されます。隔離されたファイルは、暗号化して保存されるので、コンピュータに問題を引起すことはありません。この感染ファイルが必要にな場合は、隔離領域から元の場所に戻して使用できます。

3c

感染ファイルやオブジェクトが、必要か不要がを判別できる場合には、スキャン結果 1 件ごとに操作を実行することもできます。

スキャン結果一覧の**操作**領域で、感染ファイル 1 件ごとに処理方法を決めます。

- **ログを残すのみ**: 感染したファイルをログとして記録します。感染ファイルのウイルス駆除やファイル削除はされません。※ウイルスをログに残すだけの場合、ウイルスは活動を続けるため危険です。

- **ウイルス駆除（不可能な場合はログを残すのみ）**: 感染ファイルからウイルスを駆除できない場合には、ファイルを検出時のままの状態でログに残し、このログを基に後で処理方法を決めることができます。※ウイルスをログに残すだけの場合、ウイルスは活動を続けるため危険です。

- **ウイルス駆除（不可能な場合は隔離）**: 感染ファイルからウイルスを駆除できない場合には、ファイルを検出時のままの状態でログに残し、**隔離**します（推奨設定）。隔離に関する詳細は、隔離されたファイルを参照してください。

- **ウイルス駆除（不可能な場合はファイルを削除）**: 感染ファイルからウイルスを駆除できなかった場合は、ファイルを削除します。この処理方法は、コンピュータ上に重要なデータが無い場合にのみ選択してください。※感染ファイルを完全に削除すると、場合によっては、Windows の動作に影響を与える可能性があります。対象のファイルが、削除しても問題ないファイルの時にのみ、選択してください。

- **ファイルを隔離**: 感染ファイルを暗号化して、**隔離領域**に移動します。隔離領域に移動した感染ファイルは、後で修正できるように暗号化して保管され、有害な活動ができないように暗号化されます。隔離に関する詳細は、隔離されたファイルを参照してください。

- **削除**: ファイルを削除します。※感染ファイルを完全に削除すると、場合によっては、Windows の動作に影響を与える可能性があります。対象のファイルが、削除しても問題ないファイルの時にのみ、選択してください。

［操作を実行］をクリックすると、検出されたウイルスごとに、ユーザーが設定した処理が行われます。

これでスキャン終了です。ログを残すのみにしていた検出がある場合は、マルウェアはまだコンピュータに残った状態になっていますので、ご注意ください。

ウイルス検出時の対応

ウイルスまたは他の不正プログラムが発見された場合、感染ファイルを以下の方法で処理できます。

感染ファイルにアクセスしようとした際に表示されるダイアログで、以下の処理方法を選択できます:

- **ファイルアクセスをブロック**: 感染したファイルへのアクセスをブロックします。感染ファイルのウイルス駆除やファイル削除はされません。※一時的にアクセスはブロックされますが、ウイルスはコンピュータに残るため危険です。

- **ウイルス駆除（不可能な場合はアクセスをブロック）**: 感染ファイルからウイルスを駆除できない場合には、ファイルへのアクセスをブロックします。※一時的にアクセスはブロックされますが、ウイルスはコンピュータに残るため危険です。

- **ウイルス駆除（不可能な場合は隔離）**: 感染ファイルからウイルスを駆除できない場合には、ファイルを検出時のままの状態でログに残し、隔離します（推奨設定）。隔離に関する詳細は、隔離されたファイルを参照してください。

- **ファイルを隔離**: 感染ファイルを暗号化して、**隔離領域**に移動します。隔離領域に移動した感染ファイルは、後で修正できるように暗号化して保管され、有害な活動ができないように暗号化されます。隔離に関する詳細は、隔離されたファイルを参照してください。

- **感染ファイルを削除**: ファイルを削除します。※感染ファイルを完全に削除すると、場合によっては、Windows の動作に影響を与える可能性があります。対象のファイルが、削除しても問題ないファイルの時にのみ、選択してください。

メールボックスの隔離に関しての注意: ※電子メールのメールボックス用のアーカイブは隔離しないでください。メールボックスのアーカイブ（**拡張子.pst のファイルなど**）が隔離されると、メールプログラムはメールデータにアクセスできなくなり、メールプログラムは適切に機能しなくなります。

ウイルススキャンで「not-a-virus」が表示される

「not-a-virus」 と表示されるファイルは、ファイル自身は不正機能を持っていませんが、ある状況においては攻撃者によって不正利用され、コンピュータに危害を加えられる可能性があるアプリケーションです。

not-a-virus カテゴリには、キー配列自動変更ツール、IRCクライアント、FTPサーバー、プロセス作成（または隠す）ツールなどあります。

アンインストールの方法

本製品をアンインストールする場合は、以下の手順でアンインストールが可能です。

- **Windows 8 / 8.1**: スタート画面（Modern UI）から、本製品のアイコンを右クリックし、画面下の［**アンインストール**］を選択します。表示された［**プログラムと機能**］ウインドウから、本製品を選択し、［**アンインストール**］をクリックしてアンインストールを実行します。

- **Windows Vista, Windows 7**: Windows タスクバーで **[スタート]** （通常はディスプレイの左下に配置）をクリックし、**[コントロールパネル]** を選択します。 そこで **[プログラム] > [プログラムのアンインストール]** を選択します。表示されたリストから 本製品を選択し、**[アンインストール]** をクリックしてアンインストールを実行します。

- **Windows XP**: Windows タスクバーの **[スタート]** をクリックして **[設定] > [コントロールパネル] > [プログラムの追加と削除]** を選択します。表示された **[プログラムの追加と削除]** ウインドウから、本製品をマウスで選択します。そして **[変更と削除]** をクリックしてアンインストールを実行します。

隔離済みファイルが隔離領域に残っていると、アンインストール中に、これらファイルを削除するかどうかを確認されます。隔離ファイルを削除しない場合は、当該ファイルは暗号化されてコンピュータ上に保存され、アンインストール後もコンピュータ内に残ります（これらのファイルは本製品を再インストールしないと使用できません）。また、アンインストール中に、**設定とログ**を削除するかどうかについても確認されます。これらのファイルを削除せずにコンピュータに残しておくと、ソフトウェアを再インストールした場合、保存されたログと設定が再び使用できるようになります。

［**終了**］をクリックすると、アンインストールを終了します。これでソフトウェアがシステムから完全にアンインストールされます。

USB キーボードを間違ってブロックした場合

USBキーボードガードを使用中、接続したUSBキーボードを間違ってブロックもしくは許可した場合は、以下の方法で該当キーボードの情報を削除することができます。

- **方法1**: インストールされているG DATA製品をアンインストール、再インストールすると、USBキーボードガードで設定したキーボードの情報は削除されます。
  再度USBキーボードを接続すると、USBキーボードガードのポップアップが表示されますので、そこで正しい設定を行ってください。

- **方法2（上級者向け）**: G DATA製品をインストールしたままで、レジストリエディタを使用し、以下のレジストリキーを開いてください。

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\GDKeyboard Guard

  このレジストリキー内に [HID\VID_...] で始まる値がありますので、これを削除してPCを再起動すると、USBキーボードガードで設定したキーボードの情報は削除されます。
  再度USBキーボードを接続すると、USBキーボードガードのポップアップが表示されますの

で、そこで正しい設定を行ってください。

※方法2はシステムのレジストリを編集する方法ですので、操作を間違えるとシステムの動作に影響を及ぼす可能性があります。この方法を実行する場合は、上記の説明が理解できるユーザーが実行してください。

FAQ: ライセンスについて

複数台用ライセンスを所有している場合

複数台用ライセンスをご購入いただくと、取得したライセンスと同数のコンピュータに 本製品をインストールして使用できます。1 台目のコンピュータへのインストールとインターネット更新が終了すると、メールでアクセスデータが送信されます。2 台目のコンピュータにもソフトウェアをインストールする時には、1台目の登録の際に発行されたユーザー名とパスワードを入力します。3 台目以降のコンピュータにもこの作業を繰り返します。

複数台用ライセンスの製品を複数のコンピュータで使用する際は、初回登録時にレジストレーション番号を登録して発行された、インターネット更新用の**アクセスデータ**（ユーザー名とパスワード）を、すべてのコンピュータで使用します。手順は以下のとおりです。

1 本製品を起動します。

2 セキュリティセンター画面で［**前回のワクチン更新**］をクリックし、プルダウンメニューから［**今すぐワクチン更新**］をクリックします。

3 表示されるウィンドウに、初回登録時にG DATA から送られてきたメールに記載されているアクセスデータを入力します。［OK］をクリックすると、更新ができるようになります。

※複数台用ライセンスは、1台目コンピュータでレジストレーション番号を初回登録した段階から、購入したライセンスの年数分使用できるようになります。2台目以降のコンピュータでも、その最初に登録したコンピュータと共通の期限が使用されますのでご注意ください。

例: 1年/3台版のライセンスを購入した場合
2014/7/1 に1台目のコンピュータでレジストレーション番号を初回登録、
2014/10/1 に2台目のコンピュータにアクセスデータを登録したとすると、全てのコンピュータのライセンス有効期限は、1台目のコンピュータで初回登録を行ってから1年後の 2015/7/1 までになります。
これは、もし 2015/7/1 以降に3台目のコンピュータにアクセスデータを登録しても、期限切れになる、という事も意味します。

そのため、複数台用のライセンスを使用する場合は、初回のレジストレーション番号の登録が終わり次第、速やかに残り全ての対象コンピュータでアクセスデータの登録を済ませるのが、ライセンスの効率的な使用方法となります。

ライセンスの期限が切れた場合

ライセンスの期限切れが近づくとポップアップのメッセージでお知らせします。このポップアップメッセージをクリックすると、ダイアログが開き、ここから更新の手続きを行うことができます。

> **メモ**: 法人向け販売パートナーから購入したライセンスの場合（マルチライセンス製品など）は、お買い上げいただいた販売パートナーへお問い合せください。

コンピュータを買い替えたり、クリーンインストールした場合

コンピュータを買い換えたり、クリーンインストールした場合は、本製品をコンピュータにインストールし、初回登録時に G DATA から送付されたアクセスデータを入力します。アクセスデータの入力は、**インストール**もしく**更新**の項を参照してください。

> **メモ**: ライセンスの移行には回数制限が設定されています。この回数を超えた場合は、更新期限が有効でも更新がロードできなくなりますので、ユーザーサポートに問い合わせください。

データ保護に関する声明

本ソフトウェアのデータ保護に関する声明

G DATA製品には、特定条件件下においてデータをG DATAのクラウドサーバーへ送信する保護コンポーネントが含まれています。保護コンポーネントのコア機能を正常に機能させるために必要な特定データは、常に同サーバーへ送信されます。保護コンポーネントの１つ、ウェブ保護には、ウェブサイトのアドレス送信が必須となります。また、別の保護コンポーネント、バンクガードでは、新種のバンキング系トロイの木馬の特定・削除のために、チェックサムの送信が必要となります。更に、ふるまい検知（ビヘイビアブロッカー）の機能は、クラウドからの情報を取得することにより、コンピュータをより効果的に保護できますが、これには、不審なファイルに関する特定の情報をクラウドサーバーへ送信する必要があります。

また、送信されるデータは、他のコンポーネントにおいても重要な意味を持っています。ユーザー様から送信されたデータは、G DATAのセキュリティラボで有害なファイルを検証や挙動の分析に使用されます。検証結果は、G DATAの保護コンポーネントの改善やG DATA製品のユーザーへの有害プログラムに関する情報やその影響を提供します。詳細は、マルウェア情報イニシアチブ（MII）のデータ保護に関する声明をご覧ください。なお、MIIへの参加は任意です。MIIへの参加を無効化しても、G DATAによる保護メカニズムは、その効果を制限されません。

重要：　これらの機能で収集される情報には、個人情報は含まれません。また、取得した情報を使って個人の特定を行うことはありません。

・ウェブ保護によるデータ収集

G DATA ウェブ保護とは?

インターネットには、数多くの有害サイトや詐欺サイトが存在しています。これらのサイトは、マルウェア配布や適切な保護が施されていないコンピュータを感染させるための感染経路（Drive-By-Infection）として使われており、個人情報を盗み出したり（例： PaypalやFacebookのサイトフィッシング）、スキャムなどの詐欺として使用されている可能性があります。G DATAは、有害サイトへのアクセスを遮断するブラックリストを独自に管理・保守しています。G DATAウェブ保護は、次の2種類のテクノロジーがベースとなっています。

1. HTTPスキャン。この機能は、既知の有害コードがないか、ウイルススキャナでスキャンしてHTTPトラフィックをチェックする機能です。有害コードが見つかった場合、G DATAが警告を発します。なお、警告が表示された場合、ユーザーが安全性に関する判定情報を、任意で送信できるケースがあります。

2.フィッシング保護。この機能は、リクエストされたアドレスがフィッシングサイトではないか、G DATA が管理・保守するブラックリストと照合し、フィッシングサイトであった場合は警告を発する機能です。このURLブラックリストには、無数の有害サイトや詐欺サイトの情報が保存されています。なお、フィッシング警告が表示された場合、ユーザーが安全性に関する判定情報を、任意で送信できるケースがあります。

収集される情報の種類は?

リクエスト先のウェブサイトがG DATAのURLブラックリストに存在するかチェックするため、ウェブサイトのアドレスをクラウドサーバーに送信します。

収集された情報の使用方法は?

リクエスト先のアドレスは、G DATAのデータベースに保存されますが、リクエスト送信元のユーザーもしくはPC情報は保存されません。ウェブサイトのアドレスは、まずG DATAの分析システムに転送され、次のステップで、有害もしくは不審な構成部分をチェックします。不審なウェブサイトのアドレスは、G DATAセキュリティラボの分析システムに転送されます。分析によって不審サイトと確認された場合は、このサイトはブラック

リストに追加されます。

G DATAのクラウドサーバーとリクエスト送信元コンピュータの間の接続中は、送信元コンピュータのIPアドレスが送信されますが、通常、このIPアドレス情報はG DATA側では保存されません。ウェブサイトがブロックされた場合は、IPアドレスをもとに国情報を識別しますが、IPアドレスは識別後に破棄します。そのため、G DATA側でリクエスト送信元の個人を特定することはできません。

・G DATA バンクガードによるデータ収集

G DATA バンクガードとは?

G DATA バンクガードは、ブラウザのメモリ領域が破損状況やマルウェアによる改竄など、ブラウザが暗号化された情報の送信に使用するシステムライブラリを監視する機能です。G DATA バンクガードがこの領域への攻撃を検出すると、保護メカニズムが作動し、攻撃されたブラウザを通常ステータスに戻します。その後、攻撃を引き起こした有害ファイルをシステムから見つけ出し、除去します。

収集するデータの種類は?

ブラウザのメモリが攻撃された場合、次の情報が送信されます 。

バージョン番号

- G DATA 製品および同コンポーネント
- ブラウザおよび同コンポーネント
- OS情報

チェックサム

- 攻撃元および攻撃に関わったファイル
- 削除されたファイル

匿名 GUID

- 発生した事象を特定のコンピュータを関連付けるため、コンピュータのGUID情報を取得します。なお、GUIDは同一の情報が存在する可能性は非常に低く、GUIDからコンピュータの場所や個人の特定はできません。

攻撃時のアクティビティ情報

- 攻撃を特定マルウェアに関連付けるため、攻撃種類をもとにマルウェアを特定するフィンガープリントを取得します。フィンガープリントはシステムライブラリの呼び出しに基づくもので、これには個人情報は含まれません。
- 各システムライブラリで危険にさらされている機能の名称

マルウェア除去時のアクティビティ情報

- 削除されたレジストリエントリ
- 削除時: ルートキットの種類（例： Watchdog/Versteck via Hook)

収集された情報の使用方法は?

バージョン番号は、発生した事象とプログラムバージョンを関連付けるために使用します。これは、エラー発生数の減少と脆弱なシステムの特定に役立ちます。

関連付けられたファイルのチェックサムは、G DATAのデータベース内の有害ファイルとの照合やさらに詳しい分析を行う上で、役立ちます。G DATAが保しない新たな脅威が発生した場合、この脅威は、リクエストリストへと入れられます。そして、次にこの脅威へのリクエストが確認された場合、実際にファイルが転送されます。このリクエストは、同じコンピュータから複数回送信されることはほぼありません。このリクエストは、実行可能なファイルの場合にのみ、送信されます。ドキュメント、画像、またはその他の個人情報を含むファイルなどは、送信されません。

フィンガープリントで、マルウェアを特定の系種に識別できます。同じ系種に属するマルウェアは同様の手法を用いて駆除できます。

クラウドサーバーとリクエストされたコンピュータ間の接続中は、リクエストされたコンピュータのIPアドレス情報が取得されますが、これは保存されません。ウェブサイトが有害と判定された場合、このIPアドレスを用いて、リクエスト元の国情報を取得します。このプロセスの後、IPアドレスは破棄されるため、G DATA でユーザー情報の詳細を特定することはできません。

攻撃時のアクティビティ、更に攻撃に関わったり、削除されたファイルおよびレジストリエントリの情報は、削除ルーチンの分析・開発に役立ちます。これらのデータを使うと、新たな脅威や攻撃に迅速に対応できるようになります。

特定のデータは統計に使用されます。系種別の出現頻度などはG DATAのホワイトペーパーやマルウェアレポートで使用されます。また、これらの情報は、作業プロセスの優先度の決定や自動化にも使われています。

・ふるまい検知およびファイルクラウドセキュリティによるデータ収集

ふるまい検知とは?

ふるまい検知は、コンピュータ上のすべてのアクティブなプログラムによる不審な動きを監視する機能です。ふるまい検知では、プログラムによる挙動がすべてポイントで計算され、特定の値を超えると、当該プログラムを終了に導きます。特定の条件下においては、ふるまい検知は不審なファイルのチェックサムをG DATAのサーバーへと送信し、既知のマルウェアファイルと照合します。チェックサム送信の条件は、プログラムのダウンロード時、プログラムの初回起動時、プログラムによるある程度の不審な動きが実行された場合などがあります。ファイルが有害であると判断された場合は、プログラムの実行を中止するかどうか、ユーザーに確認します。

収集するデータの種類は?

ファイルをチェックする場合、チェックサム情報を取得し、サーバーに送信します。更に、ふるまい検知が有害度評価のために取得されたパラメーター（例: 有害度（0-1）、評価したルールのID番号）が送信されます。
ファイルが有害と判定された場合、プログラムの呼び出しパラメーターが取得されます。警告メッセージに対するユーザーの操作情報も送信されます。また、ログ、ルールセット、G DATA製品のバージョン番号も送信されます。

収集された情報の使用方法は?

有害度の数値（チェックサムによって識別）は、有害なファイルをG DATAが保するマルウェアデータベースでの照合に使用します。このファイルは、ピンポイントで分析され、場合によっては、ブラックリストでブロックされます。ユーザーの操作情報は、誤検出の発見や修正に役立ちます。

・G DATA マルウェア情報イニシアチブの収集データのデータ保護に関する声明

上で述べた保護コンポーネントで必要なデータを除き、マルウェアイニシアチブでは、参加に協力頂いたユーザー様から、以下の情報を収集しています。これらの情報は、保護メカニズムの分析・開発の迅速化に役立つので、ぜひ参加にご協力ください。

G DATA マルウェア情報イニシアチブとは?

G DATA セキュリティラボでは、G DATA 製品をご利用のユーザー様を、コンピュータの安全性を脅かす脅威からから保護するため、保護・対策の研究や分析に絶え間なく励んでいます。 マルウェア研究では、マルウェアに関する情報が多ければ多いほど、効果的な保護メカニズムの開発をいち早く進めることができます。これらの情報をG DATA の研究・分析・開発に効率的に取り入れることを可能にするための取り組みが、G DATAマルウェア情報イニシアチブです。 これにより、マルウェアに関するデータをG DATAセキュリティラボに送信することができます。 より多くのユーザー様に参加頂くことで、他のG DATA製品をご利用の方々もインターネットをより安全に利用できるようになります。

収集される情報の種類は?

原則として、次の３種類のデータ収集方法があります。

1. G DATAの保護メカニズム（ウイルススキャナ、ふるまい検知、バンクガードなど）が、ユーザー様のコンピュータ上で有害ファイルが検出された場合（送信する情報は保護メカニズムによって異なります）

2. ウェブサイト上で有害なコンテンツが発見された場合

3. ユーザー様自身が任意でG DATA セキュリティラボにデータを送信した場合

ユーザー様がマルウェアファイルをG DATA セキュリティラボへ送信すると、システムは送信されるファイルのほかに、ワクチン情報、スキャンエンジンのバージョン番号、発見場所、オリジナルのファイル名、作成日という情報が一緒に送信されます。

有害なインターネットコンテンツを検出した場合は、次のデータが送信されます。

- マルウェア情報のバージョン
- G DATA 製品および使用スキャンエンジンのバージョン番号

- 使用しているOSの言語
- コンピュータのIPアドレス匿名化のためのハッシュ
- ブラウザのユーザーエージェント
- アクセスを遮断したURLと遮断した理由（マルウェアサイト、フィッシングサイトなど）
- マルウェア名

不審な実行可能ファイルが検出された際は、次の情報を取得します。また、検出したファイルは、送信することもできます。

- 有害または不審なファイルのチェックサム
- ファイルサイズ
- ファイルに署名されている場合は、証明書の情報
- 攻撃に関わった有害または不審なファイルの検出場所
- 使用しているOSの言語
- コンピュータのIPアドレス匿名化のためのハッシュ
- 攻撃後に削除されたファイルの匿名パス
- 特定の条件下（G DATAが未所の新たな脅威が発生した場合）では、攻撃に関わったファイルのダウンロードをG DATAが要求することができます。送信されるファイルは、攻撃に関わっている実行可能なファイルのみです。

重要：　収集される情報には、個人情報は含まれません。また、取得した情報を使って個人の特定を行うことはありません。

収集したデータの利用方法は?

データの処理および保存にあたっては、各国で適用されるデータ保護ならびに開示に関する法規が適用されます。 G DATAは、すべてのデータを不正アクセスから保護するため、厳重にデータを管理します。

ウェブサイトのアドレス情報は、まず選定が行われますが、有害または詐欺サイトの共通点を突き止める用途に使用されます。分析結果はURLブラックリストやG DATA の他の保護メカニズムにも反映されます。特定のデータは、統計分析や開発などに使用されます。

不審なファイルに関する情報は、G DATA で関連ファイルとの照合や有害プログラムの挙動を分析に使用します。取得した情報は、詳しい分析を行うためのベースとなる重要な要素です。目的は、保護メカニズムによる保護や駆除機能の改善となります。

有害プログラムの挙動を検証するには、有害ファイルが必要です。このため、ファイルをG DATAに送付するこ

とができます。送信するファイルは、実行可能なファイルのみです。文書やデータベースなど個人情報を含むファイルは送信されません。更に、ファイルは２つのステップを踏んで送信されます。まず、最初のステップでは、チェックサムもしくは他の共通プロパティを用い、ファイルをリクエストリストに入れられます。ファイルが再びリクエストされると、アップロードが開始されます。これが第２のステップです。このリクエストが同じコンピュータから発生するケースはほぼありません。ファイルは、その後G DATA セキュリティラボで詳しく検証されます。統計データは、優先度の決定（例：頻度が高いほど、優先的に処理）、またはG DATAが作成するレポートに活用されます。マルウェアを削除するツールも、同様となります。

データの評価はG DATAセキュリティラボ内で行われ、評価結果はITセキュリティ分野の研究事案の解明にのみ利用されます。 収集データ利用における最大目標は、安全上のリスクの研究と保護メカニズムの開発です。 収集したデータの評価結果は例えば、ブラックリストの作成、専門記事発表のための統計、セキュリティ技術用ルールの開発などに利用されます。 このイニシアチブへの参加は任意であり、参加されなくてもご利用頂く製品の機能に影響がでることはありません。 G DATAマルウェア情報イニシアチブにご参加頂くことにより、今後すべてのG DATAユーザーがコンピューターへの脅威について、より詳細な情報を得ることができるようになるとともに、ご利用のコンピュータの保護精度が向上します。

G DATA製品によるデータ収集へのご理解とマルウェア情報イニシアチブ参加へのご協力頂きますよう、何卒宜しくお願い申し上げます。

使用許諾契約・コピーライト

G DATA Software AG （以下、「G DATA」）は、本使用許諾契約書のすべての条項に同意することを条件に、本ソフトウェア（以下、「本製品」）の使用許可をユーザー（以下、「ライセンス契約者」）に保証します。本使用許諾契約書に同意することによって、ライセンス契約者とG DATAの間に法的契約が締結されます。契約書の内容をよくお読みになってから、本製品をご利用ください。本契約書の条項に同意しない場合は、インストールを中断し本製品をお使いにならないでください。

1. 定義

「定義ファイル更新」： 製品の認証後にインターネット経由で利用できる機能（例： ウイルス定義ファイル（またはワクチンとも呼ぶ）、アンチスパム用のルール、URLリストなど）

「ドキュメンテーション」： 本製品に付属する関連文書

「ライセンス文書」： ライセンス数やライセンス効期限が記されているG DATAライセンス証明書、G DATAにより発行されたライセンス文書、あるいはライセンス契約者とG DATAとの間の書面による同意書。個人版製品では、ライセンスの適用範囲はパッケージなどに記されています。

「ソフトウェア更新」： インターネット経由で利用できるソフトウェアの新しいバージョンへの更新

「ライセンス」： ソフトウェアを利用できるPC（物理および仮想）の数量。デバイスのRAMにロードもしくはハードディスクなどの記憶領域にインストールされている状態を、ライセンスが「使用されている」とみなします。

「アクセスデータ」： 本製品に含まれているレジストレーション番号、レジストレーション番号の登録後にG DATAから送信されるユーザー名およびパスワード（定義ファイル更新もしくはソフトウェア更新の実行に必要）

2. 使用権

本使用許諾契約書では、G DATAはライセンス契約者に対して、ライセンス文書に記述されているライセンスの数量と効期間で許可される限りにおいて、非独占的、限定的、かつライセンス契約者の所属企業内部での委譲可能な使用権を許諾します。ライセンス契約者は、バックアップ目的での本製品の複製する権利をします。使用権の範囲は、G DATAのライセンス文書で定義された使用期間のすべてのソフトウェア更新および定義ファイル更新に及ぶものとします。

ライセンス契約者は、契約で合意したライセンス数を最大として、本製品をコンピュータにインストールし利用できるものとします。ライセンス文書はライセンス契約者が所持するライセンス数の証明となる文書です。

ライセンス契約者は、本使用許諾契約書の許諾事項を除き、G DATAによる書面の許可なく、（i）本製品の複製、改変、レンタル、リース、サブライセンスの譲渡、または利益の取得や未取得に関わらず、その他の手段を利用して第者に本製品を譲渡、（ii）本製品をベースに派生製品を開発、（iii）リバースエンジニアリング、逆アセンブルまたは逆コンパイル、（iv）第三者へアクセスデータを開示、する権限をさないものとします。

3. 所権

本製品の所権はG DATAもしくはライセンス提供者に帰属し、本製品は著作権法およびその他の知的財産権や国際条約によって保護されています。本製品の複製、修正、拡張および同製品の関連品に関するすべての権利は、G DATAおよびライセンス提供者に帰属し、ライセンス契約者は、これに同意するものとします。上記2の条項における本製品の使用権は、製品の購入によりライセンス契約者に移ります。

4. 保証

G DATAまたは販売代理店は、本製品を記録した記憶媒体もしくはダウンロードによる配布時において、ライセンス契約者に対し、通常の操作および保守条件下においてのみ、媒体もしくはダウンロードした製品がエラーなく動作することを保証します。万一、データ媒体もしくはダウンロードした製品にエラーが存在する場合は、G DATAもしくは販売代理店の定める保証期間内であれば、購入者は代替品の引渡しを要求できるものとします。上記の保証は、事故、不正利用、許可されていない修正、変更、拡張、または不適切な利用方法に起因する損害には適用されません。

上記に明示した保証は、適用される法律の許す限りにおいて唯一かつ排他的な保証であり、特定目的や商品性の保証を含め、その他のあらゆる明示的、黙示的保証に代わるものとします。G DATAは、本製品がライセンス契約者のあらゆる要求を満たす、あるいは如何なる環境においてもエラーが生じることなく動作することを保証しかねます。G DATAおよびG DATAのライセンサー、ライセンシー、サプライヤー、または販売業者は、重大過失または明確に法律によって定義された状況を除き、本製品の使用または本ライセンス契約書に直接的または非直接的に関わらず、ライセンス契約者に生じた物質的・非物質的な損害に対し、一切の責任を負いません。なお、補償額は本製品の購入金額を限度とし、人的損害の場合は関連法規に準拠するものとします。

ライセンス契約者は、本製品の利用に関わるあらゆる法規および規定を遵守する責任を負い、本ライセンス契約書の受諾によってこれらを遵守することに同意するものとします。

5. テクニカルサポート

本製品のサポートは、G DATAもしくは販売代理店のサポートもしくはメンテナンスポリシーに準じて提供されるものとします。

6. ライセンス契約の解除

本使用許諾契約は、ライセンス契約者が本契約の条項を遵守しなかった場合、事前の通知なく自動的に失効するものとします。契約者は使用権が失効した時点で、ライセンス契約者は本製品の使用と本製品が記録された媒体を破棄するものとします。

7. 譲渡

事前にG DATAと書面同意し、ユーザーが使用許諾に同意した権利のすべてを譲渡する場合においてのみ、ライセンス契約者は、本契約で保証されている権利とライセンス契約を第者に譲渡できます。

8. ライセンス使用状況の検証

G DATAは、本製品が本使用許諾契約およびライセンス文書に準じた使用を確認するため、通常営業時間に基いた適切な事前通知および最大で1年に1回の履行頻度を条件に、G DATAが任命した守秘義務を課せられた監査人に、ユーザーの本製品に関するインストール状況とその記録の検証を依頼できるものとします。当該検証調査で発生する費用は、ライセンス契約者が使用許可されているライセンス数より5%超過したライセンスを使用している場合を除き、G DATAが負担するものとします。ライセンス契約者が許可されているライセンス数を超過して利用している場合は、ライセンス契約者は当該ライセンスの調査で発生した費用、および超過ライセンス分のライセンス料を負担するものとします。

9. 準拠法

本ライセンス契約書は、ドイツ連邦共和国の法律の解釈に従い、国際物品売買契約に関する国際連合条約の適用は除外されるものとします。本ライセンス契約で定められた一部もしくはすべての規定が無効、またはG DATAにより履行不能である場合でも、本ライセンス契約の残りの規定は引き続き拘束力をするものとします。本契約で定められた権利に対し違反が認められたにも関わらず、G DATAが権利履行を拒絶したとしても、以降の権利放棄を認めるものではありません。

10. サードパーティーのソフトウェア

本製品の一部には、オープンソースおよびフリーライセンスなどのサードパーティーにより開発されたソフトウェアが含まれています。本ライセンス契約は、上述のオープンソースおよびフリーライセンスに適用される権利または義務に対し効力を持ちません。相違する記述または異なる解釈がある場合、本ライセンス契約書の保証制限および保証排除はサードパーティーのソフトウェアに適用されます。

11. 個人情報の取り扱い

a) お客様に関する個人情報は、G DATAが必要な保護措置を講じたうえで、保、利用することにお客様は同意します。

- メールアドレス等、ユーザー登録時に届け出た事項及び、お客様から提出された問い合わせ内容およびアンケートへの回答内容等

b) G DATAが行うサービスにおいて、以下の目的のために個人情報を利用することにお客様は同意します。

- サポートサービスの提供、契約の更新案内、サービスに関する案内（セキュリティ情報等）、G DATAのパートナー他社製品の案内、各種調査、およびキャンペーン、イベントに関する案内、ベータ版テストの依頼等に関する案内

c) G DATAが前項を実施の際、秘密保持契約書を締結したうえで関連会社、販売代理店ならびに代行業者に対し個人情報を開示する場合があることにお客様は同意します。

12. その他の同意事項

本契約および本製品のライセンス文書は、ライセンス契約者とG DATAの間に締結される完全かつ排他的な同意書であり、あらゆる口頭書面による事前同意およびその他の合意における解釈に取って代わるものとします。本契約は、ライセンス契約書もしくは別途作成され、G DATAとライセンス契約者に署名されたライセンス文書もしくはその他の書面による取決めによってのみ、更できるものとします。

[G DATA – 2015/08/03, 13:09]

索引

1

2

A

B

C

E

F

G

I

M

N

O

P

S

U

W

Other